

Exhibit B

Exhibit 730-X
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Johnson

US Patent No. 7,849,020 (“Johnson”) was filed March 15, 2006 and claims priority to April 19, 2005 and to the extend the ’730 Patent is found to not be entitled to priority date earlier than its application date, therefore qualifies as prior art under at least 35 U.S.C. §§ 102(a), (b), and (e) as to the asserted claims of U.S. Pat. No. 8,352,730 (“the ’730 Patent”). Johnson, including any material incorporated by reference into Johnson, anticipates claims 1, 2, 5, 6, 8, and 9 (“the Asserted Claims”) of the ’730 Patent under 35 U.S.C. § 102. Johnson also renders obvious the Asserted Claims under 35 U.S.C. § 103, alone based on the state of the art and/or in combination with one or more references identified in Samsung’s accompanying disclosure for the ’730 Patent.¹

To the extent Plaintiff alleges that Johnson does not disclose any particular limitation of the Asserted Claims of the ’730 Patent, either expressly or inherently, it would have been obvious to a person of ordinary skill in the art as of the priority date of the ’730 Patent to modify the Johnson reference and/or to combine the teachings of the Johnson reference with other prior art references, including but not limited to the present prior art references found in Exhibits 730-A-W and 730-Y-Z and the corresponding section(s) of charts for other prior art references for the ’730 Patent in a manner that would have rendered the Asserted Claims invalid as obvious.

With respect to the obviousness of the Asserted Claims under 35 U.S.C. § 103, one or more of the principles enumerated by the United States Supreme Court in *KSR v. Teleflex*, 550 U.S. 398 (2007) apply, including: (a) combining various claimed elements known in the prior art according to known methods to yield a predictable result; and/or (b) making a simple substitution of one or more known elements for another to obtain a predictable result; and/or (c) using a known technique to improve a similar device or method in the same way; and/or (d) applying a known technique to a known device or method ready for improvement to yield a predictable result; and/or (e) choosing from a finite number of identified, predictable solutions with a reasonable expectation of success or, in other words, the solution was one which was “obvious to try”; and/or (f) a known work in one field of endeavor prompting variations of it for use either in the same field or a different field based on given design incentives or other market forces in which the variations were predictable to one of ordinary skill in the art; and/or (g) a teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill in the art to modify the prior art reference or to combine the teachings of various prior art references to arrive at the claimed invention. It therefore would have been obvious to one of ordinary skill in the art to combine the disclosures of these references in accordance with the principles and rationales set forth above.

¹ Samsung notes that Plaintiff appears in many instances to be pursuing overly broad constructions of various limitations of the asserted claims of the ’730 Patent in an effort to piece together an infringement claim where none exists and to accuse a product that does not practice the claims. This claim chart may take into account Plaintiff’s overly broad constructions of the claim limitations. Any assertion that a particular limitation is disclosed by a prior art reference may be based on Plaintiff’s apparent constructions and is not intended to be, and is not, an admission that such constructions are supportable or proper.

Exhibit 730-X
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Johnson

The citations to portions of any reference in this chart are exemplary only. For example, a citation that refers to or discusses a figure or figure item should be understood to also incorporate by reference that figure and any additional descriptions of that figure as if set forth fully therein. Samsung reserves the right to rely on the entirety of the references cited in this chart to show that the Asserted Claims are invalid. Citations presented for one claim limitation are expressly incorporated by reference into all other limitations for that claim as well as all limitations of all claims on which that claim depends. Samsung also reserves the right to rely on additional citations or sources of evidence that also may be applicable, or that may become applicable in light of claim construction, changes in Plaintiff's infringement contentions, and/or information obtained during discovery as the case progresses.

Claim	U.S. Patent No. 8,352,730	Exemplary Disclosure in Johnson
1pre	A method for verifying a user during authentication of an integrated device, comprising the steps of:	<p>Johnson discloses a method for verifying a user during authentication of an integrated device.</p> <p>For example, Johnson discloses user verification using biometric data measured locally on a portable device.</p> <p><i>See, e.g.,</i></p> <p>“A method is provided to authorize an online transaction between a purchaser and a merchant. The method includes providing, via an identity provider, verification of an identity of the purchaser. The method also includes providing, via a payment provider, verification of an ability of the purchaser to pay for the transaction, where the identity provider and the payment provider are different network entities. A computer system is also provided that can conduct an online transaction between a purchaser and a merchant providing one or more goods and/or services. The computer system includes a first node configured to provide verification of an identity of the purchaser, and a second node configured to provide verification of an ability of the purchaser to pay for the transaction, where the first node and the second node are associated with different network entities.”</p> <p><i>Johnson</i> at Abstract.</p>

Exhibit 730-X
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Johnson

1A	<p>persistently storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered;</p>	<p>Johnson renders obvious persistently storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered.</p> <p>For example, Johnson discloses persistent storage of user specific information and tokens carrying device specific information such as a SIM number. While Johnson does not disclose the use of biometric data, it would be obvious to include.</p> <p><i>See, e.g.,</i></p> <p>“In one embodiment, various elements of an online transaction are distributed over separate and independent network entities. For example, the identity provider may provide identity validation in the form of an identity token, which the merchant can use to verify the identity of the purchaser. The identity token may include one or more identity credentials of the end-user. The identity token may be issued based on the identity information provided by the end-user/purchaser, for example, the subscribe number from the SIM card, a network address (e.g., a Network Interface Card (NIC) identification, World Wide Name (WWN), etc.), login information, etc. Similarly, the payment provider may provide verification of the end-user's ability to pay in the form of a payment token. In addition, the payment provider may handle payment transactions on behalf of the purchaser in satisfaction of the purchase of goods and/or services from the merchant. The above described framework allows, inter alia, a purchaser and merchant that are strangers to conduct an online commercial transaction in an untrusted network environment in relative confidence, as discussed in further detail in the various exemplary embodiments provided below.” <i>Id.</i> at 6:7-27.</p> <p>“To obtain an identity token, end-user 140 provides identity information to identity provider 120. Identity information may include any information that</p>
----	--	---

Exhibit 730-X
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Johnson

		<p>enables the identity provider 120 to distinguish between end-user utilizing end-user computer 110 and the various other end-users to which identity provider may provide services. For example, the identity information may include a unique identifier associated with the hardware of end-user computer 110. In one embodiment, the identity information is provided by a SIM card issuing an identifier unique to the subscriber. Identity information may include providing a unique hardware number of the network interface card (NIC) of the end-user computer 110, a world wide name (WWN) or other network address of end-user computer 110 or any other means by which end-user computer 110 may be identified, including (in some embodiments) an established login name/password combination.” <i>Id.</i> at 7:57-8:4.</p>
1B	<p>wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;</p>	<p>Johnson renders obvious wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.</p> <p>Although, Johnson does not disclose the use of biometrics it would be obvious to include it in this way.</p> <p><i>See, e.g.,</i></p> <p>“The identity provider 120 may transmit the identity token to end-user computer 110 to forward to merchant 140 (step 235), and/or identity provider 120 may transmit the identity token directly to the merchant 140. Merchant 140 may then process the identity token to identify end-user and/or to verify that end-user is who he/she purports to be. The identity token may be used to authenticate certain information about the end-user that may affect the transaction. For example, the merchant 140 may provide a service that requires the end-user to be of a certain age. Identity credentials transmitted with the identity token may be used to ensure that the end-user is of the proper age and meets this requirement. Merchant 140 may have discounts for particular end-users that are frequent purchasers, or who received a coupon, promotional</p>

Exhibit 730-X
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Johnson

		<p>offer, etc. The merchant 140 may index a database of end-users to determine whether the end-user qualifies or should otherwise be specially handled based on the provided identity credentials.</p> <p>Optionally, the merchant 140 may request validation of the identity token by sending a request to the identity provider 120 (step 245). The request for validation of the identity token may include forwarding the identity token from merchant 140 to identity provider 120. Upon receiving the request for validation of the identity token, the identity provider 120 may validate the identity token, and thereby determine whether the identity token is authentic. The identity provider 120 may then forward an indication of the validity of the identity token to the merchant 140 (step 255). Alternatively, the merchant 140 may simply validate the identity token itself (step 265) (e.g., by assuming the identity token is valid or otherwise processing the token). Optionally, a response may be returned from the merchant 140 to the end-user computer 110, where the response may include a message of whether the identity token is valid, of any applicable discount or promotional offers, and/or any other type of message, as the invention is not limited in this respect (step 265).” <i>Id.</i> at 8:46-9:14.</p>
--	--	---

Exhibit 730-X
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Johnson

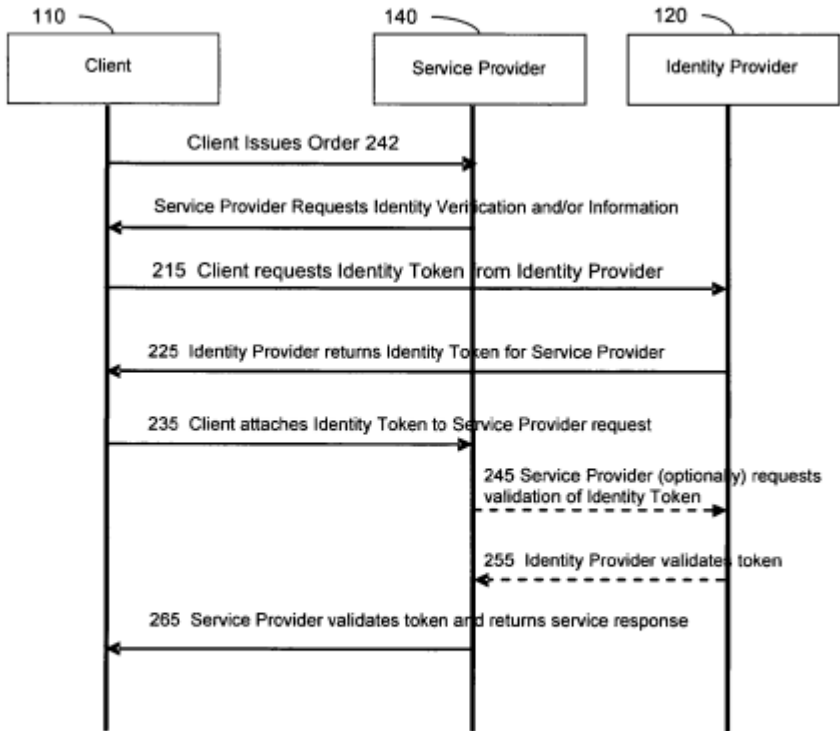
		 <pre> sequenceDiagram participant 110 as Client participant 140 as Service Provider participant 120 as Identity Provider 110->>140: Client Issues Order 242 140->>110: Service Provider Requests Identity Verification and/or Information 110->>120: 215 Client requests Identity Token from Identity Provider 120->>140: 225 Identity Provider returns Identity Token for Service Provider 110->>140: 235 Client attaches Identity Token to Service Provider request 140->>120: 245 Service Provider (optional) requests validation of Identity Token 120->>140: 255 Identity Provider validates token 140->>110: 265 Service Provider validates token and returns service response </pre> <p align="center">FIG. 2</p>
1C	responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;	<p>Johnson renders obvious responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan.</p> <p>Although, Johnson does not disclose the use of biometrics it would be obvious to include it in this way.</p>

Exhibit 730-X
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Johnson

		<p><i>See, e.g.,</i></p> <p>“The identity provider 120 may transmit the identity token to end-user computer 110 to forward to merchant 140 (step 235), and/or identity provider 120 may transmit the identity token directly to the merchant 140. Merchant 140 may then process the identity token to identify end-user and/or to verify that end-user is who he/she purports to be. The identity token may be used to authenticate certain information about the end-user that may affect the transaction. For example, the merchant 140 may provide a service that requires the end-user to be of a certain age. Identity credentials transmitted with the identity token may be used to ensure that the end-user is of the proper age and meets this requirement. Merchant 140 may have discounts for particular end-users that are frequent purchasers, or who received a coupon, promotional offer, etc. The merchant 140 may index a database of end-users to determine whether the end-user qualifies or should otherwise be specially handled based on the provided identity credentials.</p> <p>Optionally, the merchant 140 may request validation of the identity token by sending a request to the identity provider 120 (step 245). The request for validation of the identity token may include forwarding the identity token from merchant 140 to identity provider 120. Upon receiving the request for validation of the identity token, the identity provider 120 may validate the identity token, and thereby determine whether the identity token is authentic. The identity provider 120 may then forward an indication of the validity of the identity token to the merchant 140 (step 255). Alternatively, the merchant 140 may simply validate the identity token itself (step 265) (e.g., by assuming the identity token is valid or otherwise processing the token). Optionally, a response may be returned from the merchant 140 to the end-user computer 110, where the response may include a message of whether the identity token is valid, of any applicable discount or promotional offers, and/or any other type of message, as the invention is not limited in this respect (step 265).” <i>Id.</i> at 8:46-9:14.</p>
--	--	---

Exhibit 730-X
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Johnson

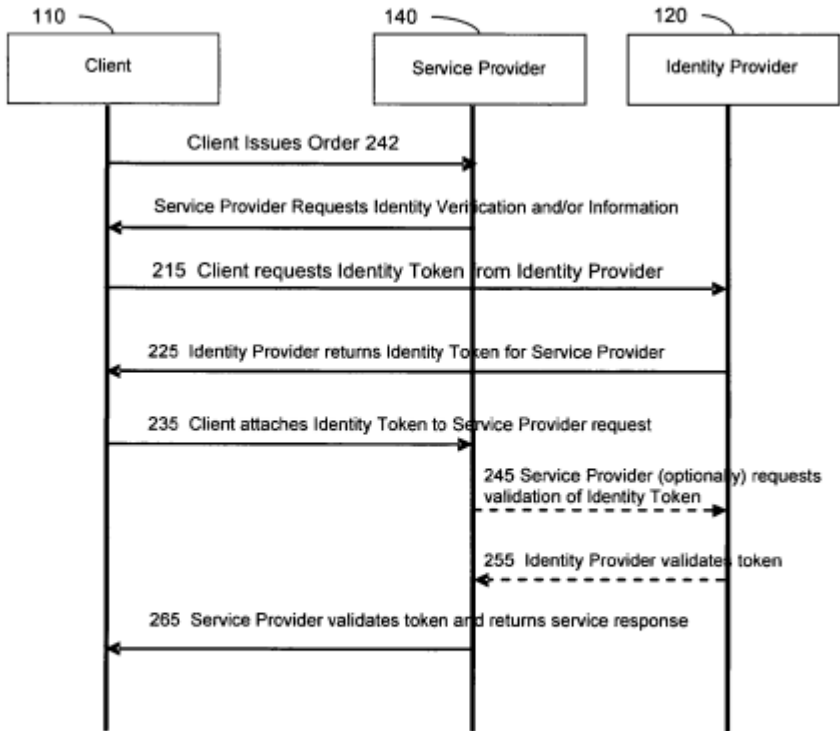
		 <pre> sequenceDiagram participant 110 as Client participant 140 as Service Provider participant 120 as Identity Provider 110->>140: Client Issues Order 242 140->>110: Service Provider Requests Identity Verification and/or Information 110->>120: 215 Client requests Identity Token from Identity Provider 120->>140: 225 Identity Provider returns Identity Token for Service Provider 110->>140: 235 Client attaches Identity Token to Service Provider request 140->>120: 245 Service Provider (optional) requests validation of Identity Token 120->>140: 255 Identity Provider validates token 140->>110: 265 Service Provider validates token and returns service response </pre> <p align="center">FIG. 2</p>
1D	<p>comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;</p>	<p>Johnson renders obvious comparing the scan data to the biometric data to determine whether the scan data matches the biometric data.</p> <p>Although, Johnson does not disclose the use of biometrics it would be obvious to include it in this way.</p>

Exhibit 730-X
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Johnson

		<p><i>See, e.g.,</i></p> <p>“The identity provider 120 may transmit the identity token to end-user computer 110 to forward to merchant 140 (step 235), and/or identity provider 120 may transmit the identity token directly to the merchant 140. Merchant 140 may then process the identity token to identify end-user and/or to verify that end-user is who he/she purports to be. The identity token may be used to authenticate certain information about the end-user that may affect the transaction. For example, the merchant 140 may provide a service that requires the end-user to be of a certain age. Identity credentials transmitted with the identity token may be used to ensure that the end-user is of the proper age and meets this requirement. Merchant 140 may have discounts for particular end-users that are frequent purchasers, or who received a coupon, promotional offer, etc. The merchant 140 may index a database of end-users to determine whether the end-user qualifies or should otherwise be specially handled based on the provided identity credentials.</p> <p>Optionally, the merchant 140 may request validation of the identity token by sending a request to the identity provider 120 (step 245). The request for validation of the identity token may include forwarding the identity token from merchant 140 to identity provider 120. Upon receiving the request for validation of the identity token, the identity provider 120 may validate the identity token, and thereby determine whether the identity token is authentic. The identity provider 120 may then forward an indication of the validity of the identity token to the merchant 140 (step 255). Alternatively, the merchant 140 may simply validate the identity token itself (step 265) (e.g., by assuming the identity token is valid or otherwise processing the token). Optionally, a response may be returned from the merchant 140 to the end-user computer 110, where the response may include a message of whether the identity token is valid, of any applicable discount or promotional offers, and/or any other type of message, as the invention is not limited in this respect (step 265).” <i>Id.</i> at 8:46-9:14.</p>
--	--	---

Exhibit 730-X
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Johnson

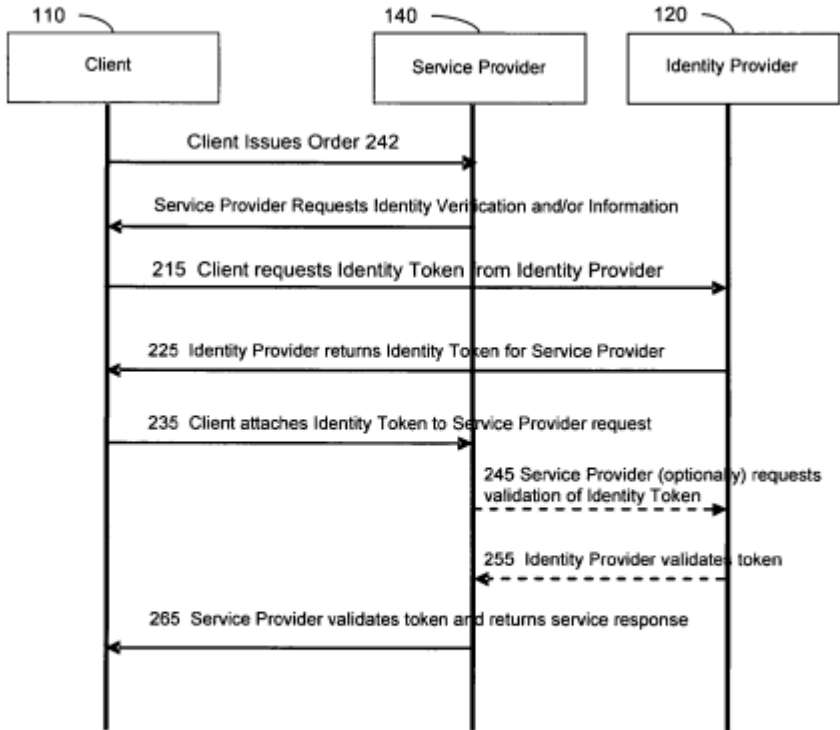
		 <pre> sequenceDiagram participant 110 as Client participant 140 as Service Provider participant 120 as Identity Provider 110->>140: Client Issues Order 242 140->>110: Service Provider Requests Identity Verification and/or Information 110->>120: 215 Client requests Identity Token from Identity Provider 120->>140: 225 Identity Provider returns Identity Token for Service Provider 110->>140: 235 Client attaches Identity Token to Service Provider request 140->>120: 245 Service Provider (optional) requests validation of Identity Token 120->>140: 255 Identity Provider validates token 140->>110: 265 Service Provider validates token and returns service response </pre> <p align="center">FIG. 2</p>
1E	responsive to a determination that the scan data matches the biometric data,	Johnson renders obvious responsive to a determination that the scan data matches the biometric data.

Exhibit 730-X
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Johnson

		<p>For example, Johnson discloses appropriately sending an identity token during a requested transaction. Although, Johnson does not disclose the use of biometrics it would be obvious to include it in this way.</p> <p><i>See, e.g.,</i></p> <p>“The identity provider 120 may transmit the identity token to end-user computer 110 to forward to merchant 140 (step 235), and/or identity provider 120 may transmit the identity token directly to the merchant 140. Merchant 140 may then process the identity token to identify end-user and/or to verify that end-user is who he/she purports to be. The identity token may be used to authenticate certain information about the end-user that may affect the transaction. For example, the merchant 140 may provide a service that requires the end-user to be of a certain age. Identity credentials transmitted with the identity token may be used to ensure that the end-user is of the proper age and meets this requirement. Merchant 140 may have discounts for particular end-users that are frequent purchasers, or who received a coupon, promotional offer, etc. The merchant 140 may index a database of end-users to determine whether the end-user qualifies or should otherwise be specially handled based on the provided identity credentials.</p> <p>Optionally, the merchant 140 may request validation of the identity token by sending a request to the identity provider 120 (step 245). The request for validation of the identity token may include forwarding the identity token from merchant 140 to identity provider 120. Upon receiving the request for validation of the identity token, the identity provider 120 may validate the identity token, and thereby determine whether the identity token is authentic. The identity provider 120 may then forward an indication of the validity of the identity token to the merchant 140 (step 255). Alternatively, the merchant 140 may simply validate the identity token itself (step 265) (e.g., by assuming the identity token is valid or otherwise processing the token).</p> <p>Optionally, a response may be returned from the merchant 140 to the end-user computer 110, where the response may include a message of whether the identity token is valid, of any applicable discount or promotional offers, and/or</p>
--	--	---

Exhibit 730-X
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Johnson

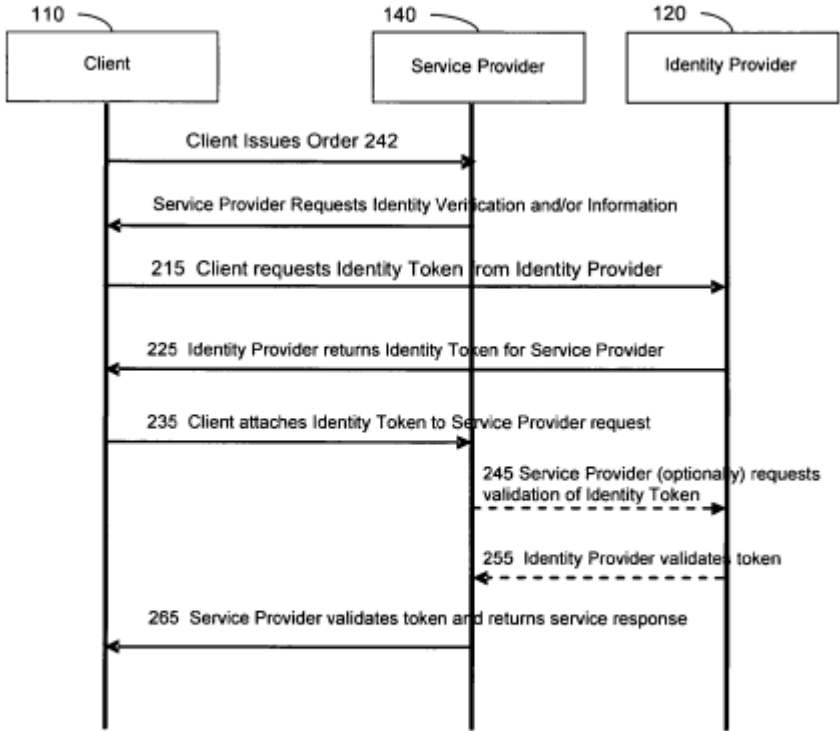
		<p>any other type of message, as the invention is not limited in this respect (step 265).” <i>Id.</i> at 8:46-9:14.</p>  <pre> sequenceDiagram participant 110 as Client participant 140 as Service Provider participant 120 as Identity Provider 110->>140: Client Issues Order 242 140->>110: Service Provider Requests Identity Verification and/or Information 110->>120: 215 Client requests Identity Token from Identity Provider 120->>140: 225 Identity Provider returns Identity Token for Service Provider 110->>140: 235 Client attaches Identity Token to Service Provider request 140->>120: 245 Service Provider (optional) requests validation of Identity Token 120->>140: 255 Identity Provider validates token 140->>110: 265 Service Provider validates token and returns service response </pre> <p align="center">FIG. 2</p>
1F	wirelessly sending one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a	Johnson discloses wirelessly sending one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying

Exhibit 730-X
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Johnson

	<p>list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values includes the device ID code; and</p>	<p>legitimate integrated devices, wherein the one or more codes and other data values includes the device ID code.</p> <p>For example, Johnson discloses sending device IDs and other information and codes to a central database for verification.</p> <p><i>See, e.g.,</i></p> <p>“An end-user computer 110 may place an order 242 with a merchant 140. The order 242 may be any indication that the end-user would like to purchase one or more goods and/or services from the merchant 140. For example, the order 242 may result from end-user selecting a good or service via a web browser displaying pages resident at the website of a merchant, or may result from choosing an option from an application running locally, as described in further detail below. As an example of the first instance, the merchant 140 may provide a website to display or otherwise offer for sale goods and/or services that it provides, or may provide an online catalog of merchandise. The order 242 may be any type of indication that end-user would like to purchase one or more goods and/or services from the merchant 140.</p> <p>As an example of the second instance and as an alternative to selecting one or more goods and services from a merchant's website, order 242 may originate from an application or other program local to the end-user computer 110. For example, an end user may create, produce or edit a document via a word processing application, design a slide show using a presentation application and/or manipulate images or graphics for a poster or brochure using an imaging application. The application may include an option under the print menu that allows the document to be printed by a third party to, for example, take advantage of printing features that may not be locally available, or to otherwise exploit professional printing services. When the option is selected, the application may send, via the network, order 242 to the merchant 140. It should be appreciated that order 242 may be any indication to purchase any good and/or service, as the aspects of the invention are not limited in this respect.</p>
--	---	--

Exhibit 730-X
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Johnson

		<p>In response to order 242, merchant 140 may request that end-user 110 provide an indication of the end-user's identity and/or verification that the end-user is indeed who he/she purports to be (step 205). For example, merchant 140 may not know anything about the source of order 242 and may desire information about the identity of the end-user and/or assurance that the end-user is not spoofing his/her identity. Alternatively, the merchant 140 may send a notice or indication that payment is required for the service and demand that a payment token be provided. To obtain a payment token, it may be necessary to first establish an identity via an identity token, as described in further detail below. In either case, end-user 110 may respond to the request by the merchant 140 by enlisting the services of identity provider 120 (step 215).” <i>Id.</i> 7:11-7:55.</p> <p>“From the perspective of the merchant, the commercial transaction is substantially risk free as the identity of the end-user and the payment verification is handled by third parties and is therefore less susceptible to fraud, spoofing and even innocent mistakes in providing personal and financial information. Therefore, merchants may be more willing to conduct online commercial transactions with unknown end-users over an untrusted network. From the perspective of the end-user, personal and financial information resides with entities either that already maintain the information and/or that the end-user has an established relationship with. Confidential personal and financial end-user information need not be provided to the merchant, mitigating the vulnerabilities of having confidential information misused or misappropriated. As a result, end-users may be more willing to conduct commercial transactions with unknown merchants without having to worry about whether the merchant is trustworthy or not.</p> <p>In some conventional commercial transaction models, identity information and payment information are input by the user and processed by either a third party or the merchant. As discussed above, these models are awkward, inefficient and time consuming for the user. In addition, conventional models present numerous issues regarding security of an end-user's confidential information as</p>
--	--	--

Exhibit 730-X
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Johnson

		<p>well as making a merchant vulnerable to fraud and/or susceptible to failure to pay by an end-user. Applicant has appreciated that commercial transaction software installed on each of the computers employed in various commercial transactions may mitigate or eliminate concerns over security and fraud. In addition, many of the actions handled by the end-user and merchant in conventional models may be performed by the commercial transactions software, making the transaction simpler and more intuitive to the end-user.” <i>Id.</i> at 10:47-11:12.</p>
1G	responsive to authentication of the one or more codes and the other data values by the agent,	<p>Johnson discloses responsive to authentication of the one or more codes and the other data values by the agent.</p> <p>For example, Johnson discloses transmitting an authentication output following verification of biometric data.</p> <p><i>See, e.g.,</i></p> <p>“The identity provider 120 may transmit the identity token to end-user computer 110 to forward to merchant 140 (step 235), and/or identity provider 120 may transmit the identity token directly to the merchant 140. Merchant 140 may then process the identity token to identify end-user and/or to verify that end-user is who he/she purports to be. The identity token may be used to authenticate certain information about the end-user that may affect the transaction. For example, the merchant 140 may provide a service that requires the end-user to be of a certain age. Identity credentials transmitted with the identity token may be used to ensure that the end-user is of the proper age and meets this requirement. Merchant 140 may have discounts for particular end-users that are frequent purchasers, or who received a coupon, promotional offer, etc. The merchant 140 may index a database of end-users to determine whether the end-user qualifies or should otherwise be specially handled based on the provided identity credentials.</p>

Exhibit 730-X
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Johnson

	<p>Optionally, the merchant 140 may request validation of the identity token by sending a request to the identity provider 120 (step 245). The request for validation of the identity token may include forwarding the identity token from merchant 140 to identity provider 120. Upon receiving the request for validation of the identity token, the identity provider 120 may validate the identity token, and thereby determine whether the identity token is authentic. The identity provider 120 may then forward an indication of the validity of the identity token to the merchant 140 (step 255). Alternatively, the merchant 140 may simply validate the identity token itself (step 265) (e.g., by assuming the identity token is valid or otherwise processing the token). Optionally, a response may be returned from the merchant 140 to the end-user computer 110, where the response may include a message of whether the identity token is valid, of any applicable discount or promotional offers, and/or any other type of message, as the invention is not limited in this respect (step 265).</p> <p>After the merchant 140 has processed the identity token and/or has received a validation for the identity token from the identity provider 120, the merchant 140 may request that the end-user provide verification or validation of an ability to pay and/or provide an indication of how the end-user would like to pay for the goods or services. The merchant 140 may make the request via a payment token request (step 305 in FIG. 3). In response to the payment token request, the end-user computer 110 may enlist the services of a payment provider 130. Payment provider 130 may be associated with a third party that maintains financial and payment information about various end-users, such as a financial institution, or a third party broker that handles financial transactions and payment procedures.</p> <p>The end-user computer 110 may solicit a payment token from a payment provider 130 (step 315) by transmitting the identity token to payment provider 130. Alternatively, the end-user may request a payment token by logging onto the payment provider 130 in a manner similar to that discussed in connection with the identity provider 120 (i.e., by providing an identifier such as a SIM subscriber number, NIC address and/or using a login/password combination). It should be appreciated that the end-user may request a payment</p>
--	---

Exhibit 730-X
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Johnson

		<p>token in other ways, as the invention is not limited in this respect. In addition, the end-user may send information about the purchase, such as the price and nature of the purchase so that the payment provider can verify that the end-user is capable of paying. However, providing purchase information is not required, as it may not be necessary or it may be handled in subsequent steps of the transaction.” <i>Id.</i> at 8:46-9:44</p> <p>“In one embodiment, the local installation of the commercial transaction software 485 a on identity provider 420 can create an identity token identifying the end-user utilizing end-user computer 410. Furthermore, the commercial transaction software 485 a on identity provider 420 can forward the identity token to the end-user computer 410, the payment provider 430, the merchant 440, and/or any other computer, as the invention is not limited in this respect. The local installation of the commercial transaction software 485 b on the end-user computer 410 can issue identity information (so as to identify the end-user) in response to an indication to conduct an online transaction between the end-user and a merchant. The local installation of the commercial transaction software 485 c installed on payment provider 430 can receive the identity token and generate a payment token verifying an ability of the end-user to pay (e.g., the payment token) for the online transaction. The local installation of the commercial transaction software 485 d installed on the merchant 440 can receive the verification of the ability of the end-user to pay before proceeding with the online transaction.</p> <p>In one embodiment, each of the computers in system 400 operates using a local installation of a same or similar operating system 495. For example, each of the computers in system 400 may operate using the Microsoft Windows® operating system. Commercial transactions software 485 may be a subsystem of the operating system. In this way, the various computers employed in a commercial transaction communicate in a consistent and known fashion. Since the commercial transactions software is communicating directly over the network and handling the validation, verification and security, the end-user and merchant need not know anything about one another, and more importantly, may not need to establish any trust relationship. In addition, because certain</p>
--	--	--

Exhibit 730-X
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Johnson

		<p>portions of the transactions are handled by the operating system, much of the transaction may be performed substantially invisible to the user, without requiring confusing and often times awkward involvement by the end-user. By having the commercial transactions software on each computer, various encryption techniques may be used during transmission of information from one computer to another. Moreover, further security features may be included such as identity tokens and/or payment tokens that are valid for a limited time period. For example, an identity token may include a time component that specifies a time after which any component receiving and processing the token should deem it invalid, and not honor the token as verification of identity and/or payment. The commercial transactions software components may programmatically process any time limits associated with a token. This may prevent tokens obtained by “fishing” from being used inappropriately at a later date.” <i>Id.</i> at 11:34-12:16</p>
1H	receiving an access message from the agent allowing the user access to an application,	<p>Johnson discloses receiving an access message from the agent allowing the user access to an application.</p> <p>For example, Johnson discloses returning results of verification process to the local device and user.</p> <p><i>See, e.g.,</i></p> <p>“The identity provider 120 may transmit the identity token to end-user computer 110 to forward to merchant 140 (step 235), and/or identity provider 120 may transmit the identity token directly to the merchant 140. Merchant 140 may then process the identity token to identify end-user and/or to verify that end-user is who he/she purports to be. The identity token may be used to authenticate certain information about the end-user that may affect the transaction. For example, the merchant 140 may provide a service that requires the end-user to be of a certain age. Identity credentials transmitted with the identity token may be used to ensure that the end-user is of the proper age and meets this requirement. Merchant 140 may have discounts for particular end-</p>

Exhibit 730-X
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Johnson

		<p>users that are frequent purchasers, or who received a coupon, promotional offer, etc. The merchant 140 may index a database of end-users to determine whether the end-user qualifies or should otherwise be specially handled based on the provided identity credentials.</p> <p>Optionally, the merchant 140 may request validation of the identity token by sending a request to the identity provider 120 (step 245). The request for validation of the identity token may include forwarding the identity token from merchant 140 to identity provider 120. Upon receiving the request for validation of the identity token, the identity provider 120 may validate the identity token, and thereby determine whether the identity token is authentic. The identity provider 120 may then forward an indication of the validity of the identity token to the merchant 140 (step 255). Alternatively, the merchant 140 may simply validate the identity token itself (step 265) (e.g., by assuming the identity token is valid or otherwise processing the token).</p> <p>Optionally, a response may be returned from the merchant 140 to the end-user computer 110, where the response may include a message of whether the identity token is valid, of any applicable discount or promotional offers, and/or any other type of message, as the invention is not limited in this respect (step 265).</p> <p>After the merchant 140 has processed the identity token and/or has received a validation for the identity token from the identity provider 120, the merchant 140 may request that the end-user provide verification or validation of an ability to pay and/or provide an indication of how the end-user would like to pay for the goods or services. The merchant 140 may make the request via a payment token request (step 305 in FIG. 3). In response to the payment token request, the end-user computer 110 may enlist the services of a payment provider 130. Payment provider 130 may be associated with a third party that maintains financial and payment information about various end-users, such as a financial institution, or a third party broker that handles financial transactions and payment procedures.</p> <p>The end-user computer 110 may solicit a payment token from a payment provider 130 (step 315) by transmitting the identity token to payment provider 130. Alternatively, the end-user may request a payment token by</p>
--	--	---

Exhibit 730-X
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Johnson

		<p>logging onto the payment provider 130 in a manner similar to that discussed in connection with the identity provider 120 (i.e., by providing an identifier such as a SIM subscriber number, NIC address and/or using a login/password combination). It should be appreciated that the end-user may request a payment token in other ways, as the invention is not limited in this respect. In addition, the end-user may send information about the purchase, such as the price and nature of the purchase so that the payment provider can verify that the end-user is capable of paying. However, providing purchase information is not required, as it may not be necessary or it may be handled in subsequent steps of the transaction.” <i>Id.</i> at 8:46-9:44</p> <p>“In one embodiment, the local installation of the commercial transaction software 485 a on identity provider 420 can create an identity token identifying the end-user utilizing end-user computer 410. Furthermore, the commercial transaction software 485 a on identity provider 420 can forward the identity token to the end-user computer 410, the payment provider 430, the merchant 440, and/or any other computer, as the invention is not limited in this respect. The local installation of the commercial transaction software 485 b on the end-user computer 410 can issue identity information (so as to identify the end-user) in response to an indication to conduct an online transaction between the end-user and a merchant. The local installation of the commercial transaction software 485 c installed on payment provider 430 can receive the identity token and generate a payment token verifying an ability of the end-user to pay (e.g., the payment token) for the online transaction. The local installation of the commercial transaction software 485 d installed on the merchant 440 can receive the verification of the ability of the end-user to pay before proceeding with the online transaction.</p> <p>In one embodiment, each of the computers in system 400 operates using a local installation of a same or similar operating system 495. For example, each of the computers in system 400 may operate using the Microsoft Windows® operating system. Commercial transactions software 485 may be a subsystem of the operating system. In this way, the various computers employed in a commercial transaction communicate in a consistent and known fashion. Since</p>
--	--	--

Exhibit 730-X
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Johnson

		<p>the commercial transactions software is communicating directly over the network and handling the validation, verification and security, the end-user and merchant need not know anything about one another, and more importantly, may not need to establish any trust relationship. In addition, because certain portions of the transactions are handled by the operating system, much of the transaction may be performed substantially invisible to the user, without requiring confusing and often times awkward involvement by the end-user. By having the commercial transactions software on each computer, various encryption techniques may be used during transmission of information from one computer to another. Moreover, further security features may be included such as identity tokens and/or payment tokens that are valid for a limited time period. For example, an identity token may include a time component that specifies a time after which any component receiving and processing the token should deem it invalid, and not honor the token as verification of identity and/or payment. The commercial transactions software components may programmatically process any time limits associated with a token. This may prevent tokens obtained by “fishing” from being used inappropriately at a later date.” <i>Id.</i> at 11:34-12:16</p>
1I	<p>wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.</p>	<p>Johnson discloses wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.</p> <p>For example, Johnson discloses use of the system with an ATM, computer, and vending machine.</p> <p><i>See, e.g.,</i></p> <p>“The end-user computer 110 may solicit a payment token from a payment provider 130 (step 315) by transmitting the identity token to payment provider 130. Alternatively, the end-user may request a payment token by logging onto the payment provider 130 in a manner similar to that discussed in</p>

Exhibit 730-X
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Johnson

		<p>connection with the identity provider 120 (i.e., by providing an identifier such as a SIM subscriber number, NIC address and/or using a login/password combination). It should be appreciated that the end-user may request a payment token in other ways, as the invention is not limited in this respect. In addition, the end-user may send information about the purchase, such as the price and nature of the purchase so that the payment provider can verify that the end-user is capable of paying. However, providing purchase information is not required, as it may not be necessary or it may be handled in subsequent steps of the transaction.” <i>Id.</i> at 9:29-44</p> <p>“In one embodiment, each of the computers in system 400 operates using a local installation of a same or similar operating system 495. For example, each of the computers in system 400 may operate using the Microsoft Windows® operating system. Commercial transactions software 485 may be a subsystem of the operating system. In this way, the various computers employed in a commercial transaction communicate in a consistent and known fashion. Since the commercial transactions software is communicating directly over the network and handling the validation, verification and security, the end-user and merchant need not know anything about one another, and more importantly, may not need to establish any trust relationship. In addition, because certain portions of the transactions are handled by the operating system, much of the transaction may be performed substantially invisible to the user, without requiring confusing and often times awkward involvement by the end-user. By having the commercial transactions software on each computer, various encryption techniques may be used during transmission of information from one computer to another. Moreover, further security features may be included such as identity tokens and/or payment tokens that are valid for a limited time period. For example, an identity token may include a time component that specifies a time after which any component receiving and processing the token should deem it invalid, and not honor the token as verification of identity and/or payment. The commercial transactions software components may programmatically process any time limits associated with a token. This may</p>
--	--	---

Exhibit 730-X
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Johnson

		prevent tokens obtained by “fishing” from being used inappropriately at a later date.” <i>Id.</i> at 11:54-12:16
2	The method of claim 1, wherein the one or more codes and the other data values are transmitted to the agent over a network.	<p>Johnson discloses the one or more codes and the other data values are transmitted to the agent over a network</p> <p>For example, Johnson discloses communication for verification over the Internet.</p> <p>“Network 105 may be any type of network in any type of configuration that interconnects and allows nodes connected to the network to communicate. Nodes or devices may be connected to the network via copper (e.g., Category 5) cable, optical connections, wireless or any combination thereof. Information may be transferred using any low level protocol such as Ethernet and/or any information protocol such as TCP/IP. The network 105 may have any number of devices connected to it and may be a trusted (e.g., intranet) or an untrusted network (e.g., LAN/WAN, Internet, etc.), or a combination of both. The computers connected to the network may be any type of device including, but not limited to, one or any combination of a mobile phone, a desktop computer, a tablet personal computer, a server, workstation, etc.” <i>Id.</i> at 6:47-60.</p>
5	The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user.	Johnson renders obvious the biometric data and the scan data are both based on a fingerprint scan by the user. Fingerprint data is the most obvious form of biometric data.
6	The method of claim 1, further comprising: establishing a secure communication channel prior to sending the one or more codes and the other data values for authentication.	<p>Johnson discloses establishing a secure communication channel prior to sending the one or more codes and the other data values for authentication.</p> <p>For example, Johnson discloses encrypted communications between the central database and verification device.</p>

Exhibit 730-X
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Johnson

		<p><i>See, e.g.,</i></p> <p>“Network 105 may be any type of network in any type of configuration that interconnects and allows nodes connected to the network to communicate. Nodes or devices may be connected to the network via copper (e.g., Category 5) cable, optical connections, wireless or any combination thereof. Information may be transferred using any low level protocol such as Ethernet and/or any information protocol such as TCP/IP. The network 105 may have any number of devices connected to it and may be a trusted (e.g., intranet) or an untrusted network (e.g., LAN/WAN, Internet, etc.), or a combination of both. The computers connected to the network may be any type of device including, but not limited to, one or any combination of a mobile phone, a desktop computer, a tablet personal computer, a server, workstation, etc.” <i>Id.</i> at 6:47-60.</p>
8pre	An integrated device for verifying a user during authentication of the integrated device, comprising:	<p>Johnson discloses an integrated device for verifying a user during authentication of the integrated device.</p> <p><i>See</i> 1pre.</p>
8A	a memory stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to the memory that is unable to be subsequently altered;	<p>Johnson discloses a memory stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to the memory that is unable to be subsequently altered.</p> <p><i>See</i> 1A.</p>
8B	wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial	Johnson discloses wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

Exhibit 730-X
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Johnson

	recognition, a signature recognition and a voice recognition;	<i>See 1B.</i>
8C	a verification unit, in communication with the memory, receives scan data from a biometric scan for comparison against the biometric data,	Johnson discloses a verification unit, in communication with the memory, receives scan data from a biometric scan for comparison against the biometric data, and if the scan data matches the biometric data. <i>See 1C-D.</i>
8D	and if the scan data matches the biometric data,	Johnson discloses if the scan data matches the biometric data. <i>See 1E.</i>
8E	wirelessly sends one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and the other data values includes the device ID code; and	Johnson discloses wirelessly sends one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and the other data values includes the device ID code. <i>See 1F.</i>
8F	responsive to the agent authenticating the one or more codes and the other data values,	Johnson discloses responsive to the agent authenticating the one or more codes and the other data values. <i>See 1G.</i>
8G	a radio frequency communicator, receives an access message from the agent allowing the user access to an application,	Johnson discloses a radio frequency communicator, receives an access message from the agent allowing the user access to an application. <i>See 1F, 1H.</i>

Exhibit 730-X
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Johnson

8H	wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.	Johnson discloses wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file. <i>See 1I.</i>
9	The integrated device of claim 8, wherein the one or more codes and the other data values are transmitted to the agent over a network.	Johnson discloses the one or more codes and the other data values are transmitted to the agent over a network. <i>See 2.</i>

Exhibit 730-Y
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Ludtke

US Patent No. 7,188,110 (“Ludtke”) was filed on December 11, 2000 and issued on March 6, 2007, and therefore qualifies as prior art under at least 35 U.S.C. §§ 102(a), (b), and (e) as to the asserted claims of U.S. Pat. No. 8,352,730 (“the ’730 Patent”). Ludtke, including any material incorporated by reference into Ludtke, anticipates claims 1, 2, 5, 6, 8, and 9 (“the Asserted Claims”) of the ’730 Patent under 35 U.S.C. § 102. Ludtke also renders obvious the Asserted Claims under 35 U.S.C. § 103, alone based on the state of the art and/or in combination with one or more references identified in Samsung’s accompanying disclosure for the ’730 Patent.¹

To the extent Plaintiff alleges that Ludtke does not disclose any particular limitation of the Asserted Claims of the ’730 Patent, either expressly or inherently, it would have been obvious to a person of ordinary skill in the art as of the priority date of the ’730 Patent to modify the Ludtke reference and/or to combine the teachings of the Ludtke reference with other prior art references, including but not limited to the present prior art references found in Exhibits 730-A-X and 730-Z and the corresponding section(s) of charts for other prior art references for the ’730 Patent in a manner that would have rendered the Asserted Claims invalid as obvious.

With respect to the obviousness of the Asserted Claims under 35 U.S.C. § 103, one or more of the principles enumerated by the United States Supreme Court in *KSR v. Teleflex*, 550 U.S. 398 (2007) apply, including: (a) combining various claimed elements known in the prior art according to known methods to yield a predictable result; and/or (b) making a simple substitution of one or more known elements for another to obtain a predictable result; and/or (c) using a known technique to improve a similar device or method in the same way; and/or (d) applying a known technique to a known device or method ready for improvement to yield a predictable result; and/or (e) choosing from a finite number of identified, predictable solutions with a reasonable expectation of success or, in other words, the solution was one which was “obvious to try”; and/or (f) a known work in one field of endeavor prompting variations of it for use either in the same field or a different field based on given design incentives or other market forces in which the variations were predictable to one of ordinary skill in the art; and/or (g) a teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill in the art to modify the prior art reference or to combine the teachings of various prior art references to arrive at the claimed invention. It therefore would have been obvious to one of ordinary skill in the art to combine the disclosures of these references in accordance with the principles and rationales set forth above.

The citations to portions of any reference in this chart are exemplary only. For example, a citation that refers to or discusses a figure or figure item should be understood to also incorporate by reference that figure and any additional descriptions of that figure as if set

¹ Samsung notes that Plaintiff appears in many instances to be pursuing overly broad constructions of various limitations of the asserted claims of the ’730 Patent in an effort to piece together an infringement claim where none exists and to accuse a product that does not practice the claims. This claim chart may take into account Plaintiff’s overly broad constructions of the claim limitations. Any assertion that a particular limitation is disclosed by a prior art reference may be based on Plaintiff’s apparent constructions and is not intended to be, and is not, an admission that such constructions are supportable or proper.

Exhibit 730-Y
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Ludtke

forth fully therein. Samsung reserves the right to rely on the entirety of the references cited in this chart to show that the Asserted Claims are invalid. Citations presented for one claim limitation are expressly incorporated by reference into all other limitations for that claim as well as all limitations of all claims on which that claim depends. Samsung also reserves the right to rely on additional citations or sources of evidence that also may be applicable, or that may become applicable in light of claim construction, changes in Plaintiff's infringement contentions, and/or information obtained during discovery as the case progresses.

Claim	U.S. Patent No. 8,352,730	Exemplary Disclosure in Ludtke
1pre	A method for verifying a user during authentication of an integrated device, comprising the steps of:	<p>Ludtke discloses a method for verifying a user during authentication of an integrated device.</p> <p>For example, Ludtke discloses authenticating a user of a transaction device.</p> <p><i>See, e.g.,</i></p> <p>“A method of identifying an authorized user with a bio metric device and enabling the authorized user to access private information over a voice network is disclosed.” Ludtke at Abstract.</p> <p>“The automation of transaction record keeping at home can be enhanced as the receipts, bills and bill paying can be maintained on the transaction device or a coupled personal computing device.” <i>Id.</i> at 4:3-6.</p> <p>“Pay per use coupons may also be easily and automatically accessed from a variety of resources stored in the card and automatically cashed in when purchases are made using the card. Electronic coupons (eCoupons) are another example of eliminating paper (i.e., eliminating paper coupons) by adding value in electronic form. Additional value comes in the form of wider methods of distribution enhancements to the user experience and/or a more efficient processing on the vendor's side. For example, while shopping, an eCoupon</p>

Exhibit 730-Y
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Ludtke

		<p>stored in the transaction device can be used to pinpoint exact items the user wishes to purchase. In addition, at checkout the coupons may be automatically credited without intervention by the user. Alternately, the user may manually convey eCoupons through bar codes or the like by manual selection of the coupons. This causes the bar codes to be presented on the display of the transaction device, which are then scanned by the POS terminal. Check out clerks and administrative personal do not have to manually handle eCoupons so processing is more accurate and efficient for both the retailer and vendor. Because they are digital in nature, eCoupons benefit from flexible distribution opportunities across all forms of media, including: Internet, digital TV/radio broadcast, and packaged recorded media such as audio/computer/DVD recorded on tape or disk and accessed later on playback. By utilizing electronic coupons, real-time tracking usage provides vendors information regarding advertising channels that are returning results as eCoupons typically contain data structures that enable tracking of this information.”</p> <p><i>Id.</i> at 4:7-35.</p> <p>“The transaction device enhances security by authenticating the user of the card prior to usage such that if a card is lost or stolen, it is useless in the hands of an unauthorized person. One means of authentication is some kind of PIN code entry. Alternately, authentication may be achieved by using more sophisticated technologies such as a biometric solution (e.g., fingerprint recognition). In addition, in one embodiment in which multiple transaction devices, e.g., a privacy card and a digital wallet, are used, it may be desirable to configure the first device to enable and program the second device in a secure manner.”</p> <p><i>Id.</i> at 4:62-5:5.</p> <p>“One embodiment of a system is illustrated in FIG. 1. In this embodiment, a transaction privacy clearing house (TPCH) 110 interfaces a user 120 and a vendor 125. In this particular embodiment, a transaction device, e.g., a privacy card 130, is used to maintain the privacy of the user while enabling the user to perform transactions. The transaction device information is provided to the</p>
--	--	--

Exhibit 730-Y
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Ludtke

		<p>TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed.”</p> <p><i>Id.</i> at 6:36-44.</p>
1A	<p>persistently storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered;</p>	<p>Ludtke discloses persistently storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered.</p> <p>For example, Ludtke discloses using transaction device information and storing fingerprint data in a tamper-proof format on the integrated transaction device.</p> <p><i>See, e.g.,</i></p> <p>“The fingerprint data entry process may be performed at least twice, to confirm that the user has entered the correct data (using the correct fingerprint). If confirmation succeeds, the device writes the fingerprint image data into write-once memory, or other memory that is protected from accidental modification.”</p> <p><i>Id.</i> at 19:35-40.</p> <p>“The privacy card records the keys in its own permanent, secure memory. Thereafter, subsequent access to the privacy card by the user requires secure exchange between the card and digital wallet.”</p> <p><i>Id.</i> at 21:46-50</p> <p>“One embodiment of a system is illustrated in FIG. 1. In this embodiment, a transaction privacy clearing house (TPCH) 110 interfaces a user 120 and a vendor 125. In this particular embodiment, a transaction device, e.g., a privacy card 130, is used to maintain the privacy of the user while enabling the user to perform transactions. The transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed.”</p>

Exhibit 730-Y
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Ludtke

		<i>Id.</i> at 6:36-44.
1B	wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;	<p>Ludtke discloses wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.</p> <p>For example, Ludtke discloses a number of different types of biometric information that may be used to secure the device.</p> <p><i>See, e.g.,</i></p> <p>“Alternately, authentication may be achieved by using more sophisticated technologies such as a biometric solution (e.g., fingerprint recognition).” <i>Id.</i> at 4:65-5:1.</p> <p>“In one embodiment, fingerprint recognition is used as a security mechanism that limits access to the card 705 to authorized users. A fingerprint touch pad and associated logic 730 is therefore included in one embodiment to perform these functions. Alternately, security may be achieved using a smart card chip interface 750, which uses known smart card technology to perform the function.” <i>Id.</i> at 12:23-29.</p> <p>“FIG. 24 illustrates one embodiment of the system being utilized in a telephony based application. A standard telephone 2402 is interfaced via a telephone cable to, for example, a PBX, etc. The biometric device 2404 is integrated into the telephone 2402. In one example of operation, the user of the telephone 2402 is identified by the biometric device 2404 as an authorized user. Once identified as an authorized user, the biometric device 2404, may for example allow the user to use the telephone 2402. In another example, the biometric device 2404 may, once an authorized user is identified, allow transmission of tones representing such things as telephone numbers, access codes, PINs, etc.</p>

Exhibit 730-Y
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Ludtke

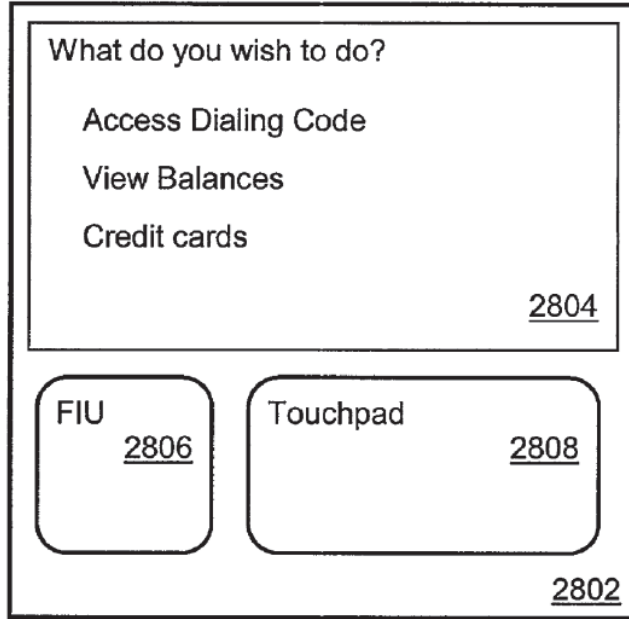
		<p>The identification by the biometric device may be achieved in a variety of ways, as discussed above. For example, biometric identification, may be, fingerprint, retinal scan, voice, DNA, hand profile, face recognition, etc.” <i>Id.</i> at 35:49-64.</p>
1C	<p>responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;</p>	<p>Ludtke discloses responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan.</p> <p>For example, Ludtke discloses using biometric verification – including a fingerprint – to verify the user of the device.</p> <p><i>See, e.g.,</i></p>  <p style="text-align: center;">FIG. 28</p> <p><i>Id.</i> at Fig. 28.</p>

Exhibit 730-Y
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Ludtke

“FIG. 28 illustrates one embodiment of a device, as a consumer access device, 2802 that implements the method discussed above. The consumer access device 2802 has an LCD screen 2804 showing text, a biometric identification unit, in this embodiment as a Fingerprint Identification Unit (FIU) 2806 and a touchpad 2808 for user input. The user of the consumer access device 2802 would be authorized access to the device 2802 if the device recognized the user after the user had pressed his finger against the FIU 2806.”

Id. at 39:19-27.

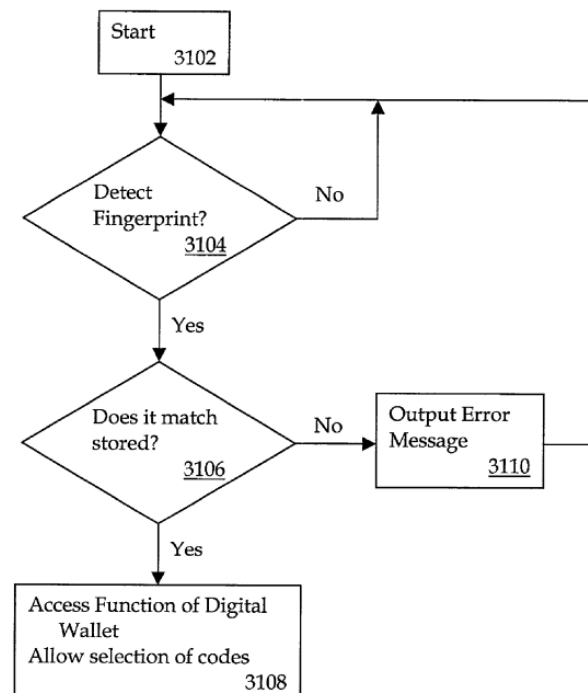


FIG. 31

Id. at Fig. 31.

Exhibit 730-Y
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Ludtke

		<p>“FIG. 31 illustrates one embodiment of a method to securely and conveniently store and transmit telephony-based data. At 3102 the user may start a device, such as a digital wallet (DW). At 3104 the DW checks to see if a fingerprint has been detected. If not then the DW loops back looking for a fingerprint. If a fingerprint has been detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint. If a match does not occur, then at 3110 an error message is output and the DW returns to checking to see if a fingerprint has been detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes.” <i>Id.</i> at 39:47-59.</p>
1D	comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;	<p>Ludtke discloses comparing the scan data to the biometric data to determine whether the scan data matches the biometric data.</p> <p>For example, Ludtke discloses comparing biometric input of user with an existing record.</p> <p><i>See, e.g.,</i></p>

Exhibit 730-Y
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Ludtke

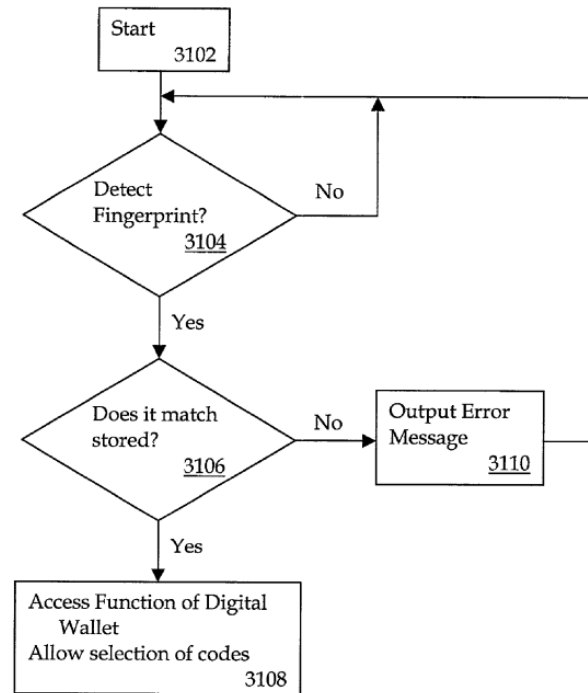


FIG. 31

Id. at Fig. 31.

“FIG. 31 illustrates one embodiment of a method to securely and conveniently store and transmit telephony-based data. At 3102 the user may start a device, such as a digital wallet (DW). At 3104 the DW checks to see if a fingerprint has been detected. If not then the DW loops back looking for a fingerprint. If a fingerprint has been detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint. If a match does not occur, then at 3110 an error message is output and the DW returns to checking to see if a fingerprint has been detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes.”

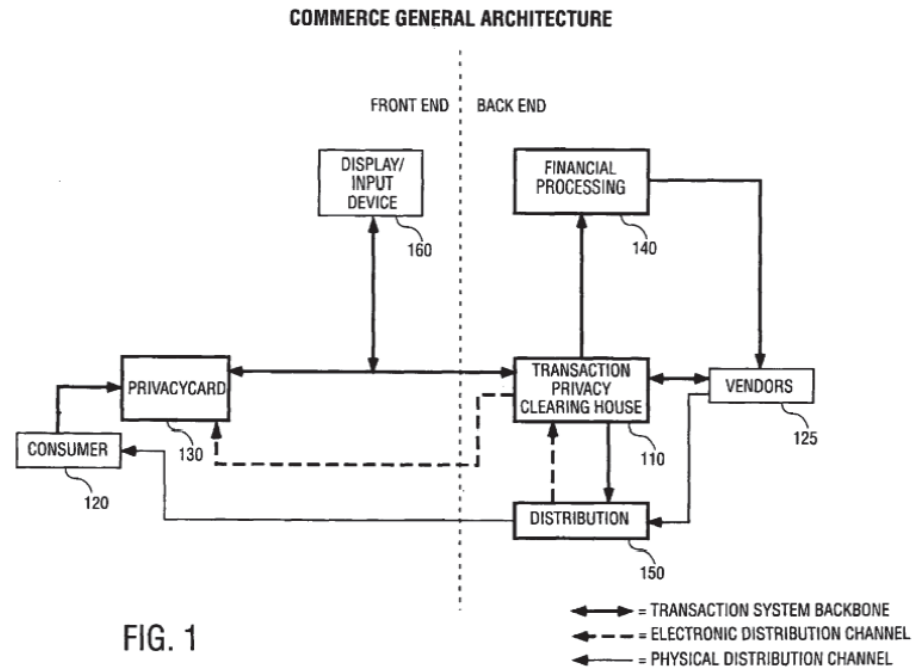
Exhibit 730-Y
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Ludtke

		<i>Id.</i> at 39:47-59.
1E	responsive to a determination that the scan data matches the biometric data,	<p>Ludtke discloses responsive to a determination that the scan data matches the biometric data.</p> <p>For example, Ludtke discloses taking action only if acquired biometric data matches the stored biometric template.</p> <p><i>See, e.g.,</i></p> <pre> graph TD Start[Start 3102] --> Detect{Detect Fingerprint? 3104} Detect -- No --> Start Detect -- Yes --> Match{Does it match stored? 3106} Match -- No --> Error[Output Error Message 3110] Error --> Start Match -- Yes --> Access[Access Function of Digital Wallet Allow selection of codes 3108] </pre> <p align="center">FIG. 31</p> <p><i>Id.</i> at Fig. 31.</p>

Exhibit 730-Y
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Ludtke

		<p>“FIG. 31 illustrates one embodiment of a method to securely and conveniently store and transmit telephony-based data. At 3102 the user may start a device, such as a digital wallet (DW). At 3104 the DW checks to see if a fingerprint has been detected. If not then the DW loops back looking for a fingerprint. If a fingerprint has been detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint. If a match does not occur, then at 3110 an error message is output and the DW returns to checking to see if a fingerprint has been detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes.” <i>Id.</i> at 39:47-59.</p>
1F	wirelessly sending one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values includes the device ID code; and	<p>Ludtke discloses wirelessly sending one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values includes the device ID code.</p> <p>For example, Ludtke discloses sending transaction device information to a transaction processing [or privacy] clearing house (TCPH) which maintains a secure database of transaction device information and user information.</p> <p><i>See, e.g.,</i></p>

Exhibit 730-Y
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Ludtke



Id. at Fig. 1.

“One embodiment of a system is illustrated in FIG. 1. In this embodiment, a transaction privacy clearing house (TPCH) 110 interfaces a user 120 and a vendor 125. In this particular embodiment, a transaction device, e.g., a privacy card 130, is used to maintain the privacy of the user while enabling the user to perform transactions. The transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed.”

Id. at 6:36-44.

“In one embodiment of electronic distribution, the TPCH 110 functions as the middleman of the distribution channel. This allows the TPCH 110 to retain user

Exhibit 730-Y
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Ludtke

		<p>privacy by not exposing addressing information and possibly email addresses to third parties.” <i>Id.</i> at 7:44-48.</p> <p>“The TPCCH 110 maintains a secure database of transaction device information and user information. In one embodiment, the TPCCH 110 interfaces to at least one financial processing system 140 to perform associated financial transactions, such as confirming sufficient funds to perform the transaction, and transfers to the vendor 125 the fees required to complete the transaction.” <i>Id.</i> at 6:49-55.</p> <p>“In one embodiment, the transaction device may be configured to closely resemble a standard credit card. More particularly, the card may have a magnetic stripe or a smart card chip that functions similarly to standard credit cards. In addition, the transaction device may contain wireless data communication, data storage and communication protocols for selectively communicating with outside devices such as a digital wallet described herein, point of sale (POS) terminal or personal computer (PC) and digital televisions (DTV).” <i>Id.</i> at 5:36-44.</p> <p>“A variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc.” <i>Id.</i> at 9:39-42.</p>
1G	responsive to authentication of the one or more codes and the other data values by the agent,	<p>Ludtke discloses responsive to authentication of the one or more codes and the other data values by the agent.</p> <p>For example, Ludtke discloses transmitting a signal (or a notification) from the TPCCH to the transaction device when device information is confirmed.</p> <p><i>See, e.g.,</i></p>

Exhibit 730-Y
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Ludtke

“The transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed.”

Id. at 6:41-44.

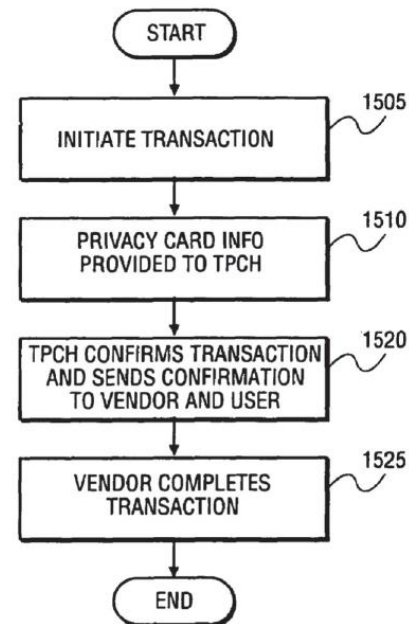


FIG. 15

Id. at Fig. 15.

“The TPCH, at step 1520, confirms the transaction and provides the confirmation to the vendor and the user. At step 1525 the vendor completes the transaction without knowledge of the identity of the user.”

Id. at 27:13-16.

Exhibit 730-Y
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Ludtke

1H	receiving an access message from the agent allowing the user access to an application,	<p>Ludtke discloses receiving an access message from the agent allowing the user access to an application.</p> <p>For example, Ludtke discloses transmitting a signal (or a notification) from the TPCCH to the transaction device when device information is confirmed.</p> <p><i>See, e.g.,</i></p> <p>“The transaction device information is provided to the TPCCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed.”</p> <p><i>Id.</i> at 6:41-44.</p>
----	--	--

Exhibit 730-Y
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Ludtke

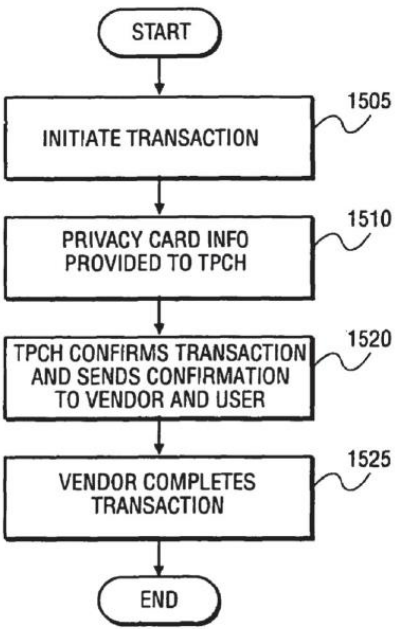
		 <p align="center">FIG. 15</p> <p><i>Id.</i> at Fig. 15.</p> <p>“The TPC, at step 1520, confirms the transaction and provides the confirmation to the vendor and the user. At step 1525 the vendor completes the transaction without knowledge of the identity of the user.”</p> <p><i>Id.</i> at 27:13-16.</p>
1I	wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.	Ludtke discloses wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

Exhibit 730-Y
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Ludtke

For example, Ludtke discloses that access would be given applications of either computer software, a file (or both).

See, e.g.,

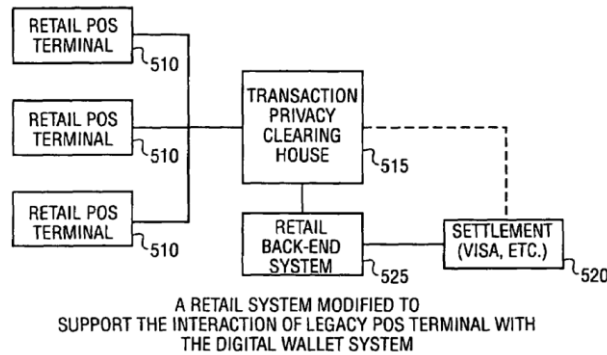


FIG. 5A

Id. at Fig. 5A.

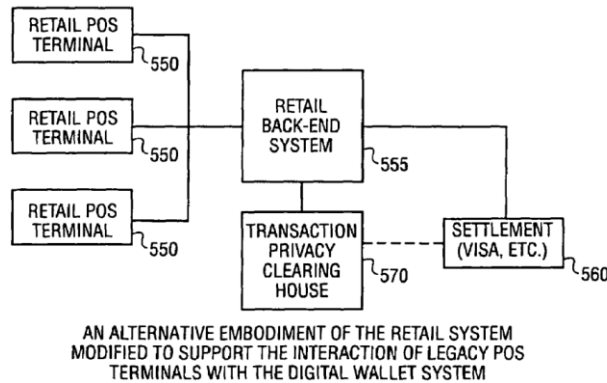


FIG. 5B

Id. at Fig. 5B.

Exhibit 730-Y
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Ludtke

		<p>“As noted above, it is contemplated that the transaction device would operate in a home environment as well as in a retail environment. FIG. 5 a is a simplified block diagram of a retail system modified to support the interaction of a legacy POS terminal with a transaction device. The terminal 510 interfaces to TPC 515 which communicates with the financial provider, for example, a credit card company 520, and the particular retailer 525. Alternately, as shown in FIG. 5 b, the POS terminal 550 interfaces to the retail system 555, which then interfaces with the credit card company 560 and the TPC 570.</p> <p>It is contemplated that the transaction device will be compatible with a variety of eCommerce system's POS terminals and therefore will provide magnetic stripe, barcode information and/or smart card chip. The magnetic stripe on the card or digital wallet can be programmed to represent a new account; thus a single transaction device may be configured to represent a number of different accounts.”</p> <p><i>Id.</i> at 9:7-25.</p>
2	The method of claim 1, wherein the one or more codes and the other data values are transmitted to the agent over a network.	<p>Ludtke discloses the one or more codes and the other data values are transmitted to the agent over a network</p> <p>For example, Ludtke discloses transmitting transaction device information over the Internet.</p> <p><i>See, e.g.,</i></p> <p>“The transaction device information is provided to the TPC 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed.”</p> <p><i>Id.</i> at 6:41-44.</p> <p>“In one embodiment, the transaction device may be configured to closely resemble a standard credit card. More particularly, the card may have a magnetic stripe or a smart card chip that functions similarly to standard credit cards. In addition, the transaction device may contain wireless data</p>

Exhibit 730-Y
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Ludtke

		<p>communication, data storage and communication protocols for selectively communicating with outside devices such as a digital wallet described herein, point of sale (POS) terminal or personal computer (PC) and digital televisions (DTV).” <i>Id.</i> at 5:36-44.</p> <p>“A variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc.” <i>Id.</i> at 9:39-42.</p>
5	The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user.	<p>Ludtke discloses the biometric data and the scan data are both based on a fingerprint scan by the user.</p> <p><i>See,</i></p> <p>“The identification by the biometric device may be achieved in a variety of ways, as discussed above. For example, biometric identification, may be, fingerprint, retinal scan, voice, DNA, hand profile, face recognition, etc.” <i>Id.</i> at 35:60-64.</p>
6	The method of claim 1, further comprising: establishing a secure communication channel prior to sending the one or more codes and the other data values for authentication.	<p>Ludtke discloses establishing a secure communication channel prior to sending the one or more codes and the other data values for authentication.</p> <p>For example, Ludtke discloses a security management function for secure communications between the transaction device and TPCH.</p> <p><i>See, e.g.,</i></p>

Exhibit 730-Y
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Ludtke

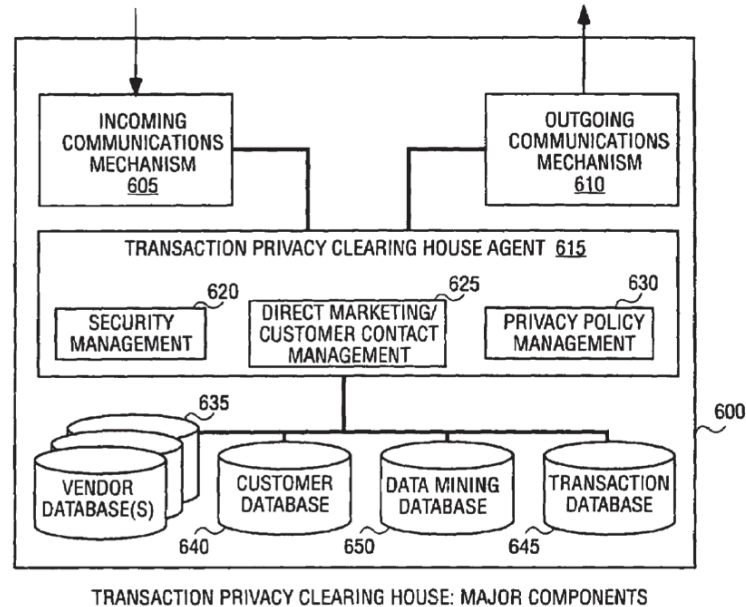


FIG. 6

Id. at Fig. 6.

“The security management function 620 ensures secure communications among the components internal to the TPC 600 and the entities external to the TPC 600. This function includes participating in secure communications protocols to open and maintain secure connections. This ensures that only authorized entities are allowed access to data and that only authorized transaction devices can execute transactions against a user's account.”

Id. at 9:52-59

Exhibit 730-Y
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Ludtke

8pre	An integrated device for verifying a user during authentication of the integrated device, comprising:	Ludtke discloses an integrated device for verifying a user during authentication of the integrated device. <i>See 1pre.</i>
8A	a memory stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to the memory that is unable to be subsequently altered;	Ludtke discloses a memory stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to the memory that is unable to be subsequently altered. <i>See 1A.</i>
8B	wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;	Ludtke discloses wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition. <i>See 1B.</i>
8C	a verification unit, in communication with the memory, receives scan data from a biometric scan for comparison against the biometric data,	Ludtke discloses a verification unit, in communication with the memory, receives scan data from a biometric scan for comparison against the biometric data, and if the scan data matches the biometric data. <i>See 1C-D.</i>
8D	and if the scan data matches the biometric data,	Ludtke discloses if the scan data matches the biometric data. <i>See 1E.</i>

Exhibit 730-Y
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Ludtke

8E	wirelessly sends one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and the other data values includes the device ID code; and	Ludtke discloses wirelessly sends one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and the other data values includes the device ID code. <i>See 1F.</i>
8F	responsive to the agent authenticating the one or more codes and the other data values,	Ludtke discloses responsive to the agent authenticating the one or more codes and the other data values. <i>See 1G.</i>
8G	a radio frequency communicator, receives an access message from the agent allowing the user access to an application,	Ludtke discloses a radio frequency communicator, receives an access message from the agent allowing the user access to an application. <i>See 1F, 1H.</i>
8H	wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.	Ludtke discloses wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file. <i>See 1I.</i>
9	The integrated device of claim 8, wherein the one or more codes and the other data values are transmitted to the agent over a network.	Ludtke discloses the one or more codes and the other data values are transmitted to the agent over a network. <i>See 2.</i>

Exhibit 730-Z
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Okereke

US Patent Publication No. 2003/0196084 (“Okereke”) was filed on April 11, 2003 and published on October 16, 2003, and therefore qualifies as prior art under at least 35 U.S.C. §§ 102(a), (b), and (e) as to the asserted claims of U.S. Pat. No. 8,352,730 (“the ’730 Patent”). Okereke, including any material incorporated by reference into Okereke, anticipates claims 1, 2, 5, 6, 8, and 9 (“the Asserted Claims”) of the ’730 Patent under 35 U.S.C. § 102. Okereke also renders obvious the Asserted Claims under 35 U.S.C. § 103, alone based on the state of the art and/or in combination with one or more references identified in Samsung’s accompanying disclosure for the ’730 Patent.¹

To the extent Plaintiff alleges that Okereke does not disclose any particular limitation of the Asserted Claims of the ’730 Patent, either expressly or inherently, it would have been obvious to a person of ordinary skill in the art as of the priority date of the ’730 Patent to modify the Okereke reference and/or to combine the teachings of the Okereke reference with other prior art references, including but not limited to the present prior art references found in Exhibits 730-A-Y and the corresponding section(s) of charts for other prior art references for the ’730 Patent in a manner that would have rendered the Asserted Claims invalid as obvious.

With respect to the obviousness of the Asserted Claims under 35 U.S.C. § 103, one or more of the principles enumerated by the United States Supreme Court in *KSR v. Teleflex*, 550 U.S. 398 (2007) apply, including: (a) combining various claimed elements known in the prior art according to known methods to yield a predictable result; and/or (b) making a simple substitution of one or more known elements for another to obtain a predictable result; and/or (c) using a known technique to improve a similar device or method in the same way; and/or (d) applying a known technique to a known device or method ready for improvement to yield a predictable result; and/or (e) choosing from a finite number of identified, predictable solutions with a reasonable expectation of success or, in other words, the solution was one which was “obvious to try”; and/or (f) a known work in one field of endeavor prompting variations of it for use either in the same field or a different field based on given design incentives or other market forces in which the variations were predictable to one of ordinary skill in the art; and/or (g) a teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill in the art to modify the prior art reference or to combine the teachings of various prior art references to arrive at the claimed invention. It therefore would have been obvious to one of ordinary skill in the art to combine the disclosures of these references in accordance with the principles and rationales set forth above.

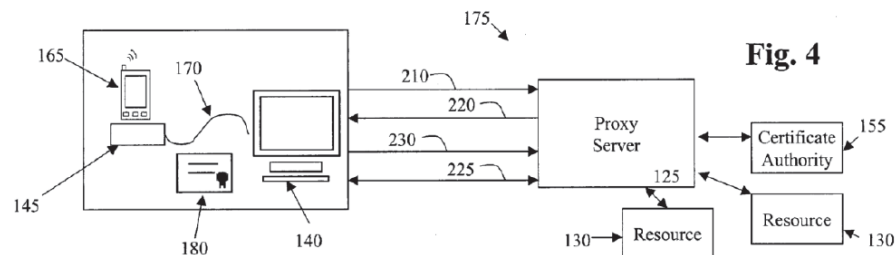
¹ Samsung notes that Plaintiff appears in many instances to be pursuing overly broad constructions of various limitations of the asserted claims of the ’730 Patent in an effort to piece together an infringement claim where none exists and to accuse a product that does not practice the claims. This claim chart may take into account Plaintiff’s overly broad constructions of the claim limitations. Any assertion that a particular limitation is disclosed by a prior art reference may be based on Plaintiff’s apparent constructions and is not intended to be, and is not, an admission that such constructions are supportable or proper.

Exhibit 730-Z**Invalidity Chart for U.S. Patent No. 8,352,730 In View of Okereke**

The citations to portions of any reference in this chart are exemplary only. For example, a citation that refers to or discusses a figure or figure item should be understood to also incorporate by reference that figure and any additional descriptions of that figure as if set forth fully therein. Samsung reserves the right to rely on the entirety of the references cited in this chart to show that the Asserted Claims are invalid. Citations presented for one claim limitation are expressly incorporated by reference into all other limitations for that claim as well as all limitations of all claims on which that claim depends. Samsung also reserves the right to rely on additional citations or sources of evidence that also may be applicable, or that may become applicable in light of claim construction, changes in Plaintiff's infringement contentions, and/or information obtained during discovery as the case progresses.

Claim	U.S. Patent No. 8,352,730	Exemplary Disclosure in Okereke
1pre	A method for verifying a user during authentication of an integrated device, comprising the steps of:	<p>Okereke discloses a method for verifying a user during authentication of an integrated device.</p> <p>For example, Okereke discloses authenticating wireless and mobile devices which are integrated devices and verifying their users.</p> <p><i>See, e.g.,</i></p> <p>“A system and method for allowing users of wireless and mobile devices to participate in Public Key Infrastructure facilitates secure remote communications. The present invention allows wireless devices to participate in secure communications with secure networks without storing compromisable information on the wireless device. In one embodiment, the system allows wireless devices to participate in Public Key Infrastructure wherein no portion of the certificate, no information about the certificate, and no private or public key data are stored on the wireless device. In one embodiment, a certificate proxy server maintains the digital certificate and private for the client device in a secure fashion, and maintains connectivity with the wireless network. The mobile user can authenticate with the server in order to access resources that require the certificate to be presented.”</p> <p>Okereke at Abstract.</p>

Exhibit 730-Z
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Okereke



Id. at Fig. 4.

“The establishment of mobile access to secure resources in accordance with the present invention can occur as shown in FIGS. 4 and 5. The proxy server can be provided with software designed in accordance with the present invention, and a thin client application can be installed and/or downloaded onto the user's desktop computer. The proxy server program then awaits the initiation of a request 210 from the desktop to establish secure wireless access capabilities using the system of the present invention. In so doing, a unique identifier for the wireless product to be employed is passed as at 210 to the proxy server 125 program for authorization. The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other device capable of remote wireless communication. The unique identifier can be a serial number or SIM. number, for example.”

Id. at ¶25.

“In other cases, an additional form of authentication may be required, such as a user name and password, a smart card, or a fingerprint, for example.”

Id. at ¶21.

“The credential information or authentication measure can be something the user has (such as a swipe card), something the user is (such as represented by a fingerprint scan), or something the user knows (such as a password or pass phrase)”

Id. at ¶26.

Exhibit 730-Z
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Okereke

1A	<p>persistently storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered;</p>	<p>Okereke discloses persistently storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered.</p> <p>For example, Okereke discloses a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device in the form of a serial number or SIM number and a a private/public key process.</p> <p><i>See, e.g.,</i></p> <p>“The establishment of mobile access to secure resources in accordance with the present invention can occur as shown in FIGS. 4 and 5. The proxy server can be provided with software designed in accordance with the present invention, and a thin client application can be installed and/or downloaded onto the user's desktop computer. The proxy server program then awaits the initiation of a request 210 from the desktop to establish secure wireless access capabilities using the system of the present invention. In so doing, a unique identifier for the wireless product to be employed is passed as at 210 to the proxy server 125 program for authorization. The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other device capable of remote wireless communication. The unique identifier can be a serial number or SIM. number, for example. If the unique identifier is one which the proxy server program identifies as being acceptable, the proxy server program will send approval as at 220 to the desktop 140, which executes functionality to make a key exchange as at 225, such as, for example, a Diffie Hellman Key Exchange. This key is used to encrypt information sent to the server using AES (Advanced Encryption Standard). AES is an encryption algorithm used by U.S. government agencies for securing sensitive but unclassified communications. In the preferred embodiment, this key is used to encrypt communication between the desktop and the server. In another embodiment, this key is used as part of a shared secret between the server and the client. This shared secret is used to</p>
----	--	--

Exhibit 730-Z
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Okereke

		<p>generate a session key. The new session key ensures that conversations cannot be eavesdropped if the key has been compromised. The shared secret eliminates the possibility of a man-in-the-middle attack.” <i>Id.</i> at ¶25.</p> <p>“The desktop computer includes a memory, processor, user interface, keyboard and mouse as is commonly known, and is preferably connected to a local area network (LAN) 175 for communication and use of shared resources as is commonly known. The user may be provided with a system PKI certificate 180 and private key for use with the desktop computer, in order to access and communicate to the extent authorized by the network administrator.” <i>Id.</i> at ¶24.</p>
1B	wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;	<p>Okereke discloses wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.</p> <p>For example, Okereke using fingerprint to secure the device.</p> <p><i>See, e.g.,</i></p> <p>“In other cases, an additional form of authentication may be required, such as a user name and password, a smart card, or a fingerprint, for example.” <i>Id.</i> at ¶21.</p> <p>“The credential information or authentication measure can be something the user has (such as a swipe card), something the user is (such as represented by a fingerprint scan), or something the user knows (such as a password or pass phrase)” <i>Id.</i> at ¶26.</p>
1C	responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;	<p>Okereke discloses responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan.</p>

Exhibit 730-Z
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Okereke

		<p>For example, Okereke discloses using biometric verification – including a fingerprint – to verify the user of the device.</p> <p><i>See, e.g.,</i></p> <p>“The wireless device 165 is provided with a memory, processor, and input/output means as is commonly known. Using the session key, the user can then encrypt credential information, its PKI certificate 180 and private key, and forward this information to the proxy server 125 as at 230 in FIGS. 4 and 5. In one embodiment of the invention, the encrypted information is sent to the proxy server via secure IP network. The credential information or authentication measure can be something the user has (such as a swipe card), something the user is (such as represented by a fingerprint scan), or something the user knows (such as a password or pass phrase). In one embodiment, the credential information is a user name and password. In another embodiment of the invention, the credential information is a random number generated by programming on the wireless device, wherein the number changes in predetermined time intervals and is synchronized with programming on the proxy server so as to always match the corresponding number maintained on the proxy server.”</p> <p><i>Id.</i> at ¶26.</p> <p>“In one embodiment of the invention, desktop software is used to authenticate the user to the CPS, register the wireless device with the CPS, facilitate the initial key exchange and transfer the certificate and private key to the server. When the user wishes to access a resource from the wireless device outside of the secure network demarcation line (102 in FIG. 3), they are prompted for a second means of authentication, which may be something the user has (such as a swipe card, synchronized password keychain or channel key, for example), something the user is (such as a fingerprint scan), or something the user knows (such as a password or pass phrase). In a preferred embodiment this second form of authentication is something the user knows. The CPS verifies both forms of authentication, locates the user's certificate and establishes a session.”</p>
--	--	---

Exhibit 730-Z
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Okereke

		<i>Id.</i> at ¶32.
1D	comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;	<p>Okereke discloses comparing the scan data to the biometric data to determine whether the scan data matches the biometric data.</p> <p>For example, Okereke discloses using biometric verification – including a fingerprint – to verify the user of the device.</p> <p><i>See, e.g.,</i></p> <p>“The wireless device 165 is provided with a memory, processor, and input/output means as is commonly known. Using the session key, the user can then encrypt credential information, its PKI certificate 180 and private key, and forward this information to the proxy server 125 as at 230 in FIGS. 4 and 5. In one embodiment of the invention, the encrypted information is sent to the proxy server via secure IP network. The credential information or authentication measure can be something the user has (such as a swipe card), something the user is (such as represented by a fingerprint scan), or something the user knows (such as a password or pass phrase). In one embodiment, the credential information is a user name and password. In another embodiment of the invention, the credential information is a random number generated by programming on the wireless device, wherein the number changes in predetermined time intervals and is synchronized with programming on the proxy server so as to always match the corresponding number maintained on the proxy server.”</p> <p><i>Id.</i> at ¶26.</p> <p>“In one embodiment of the invention, desktop software is used to authenticate the user to the CPS, register the wireless device with the CPS, facilitate the initial key exchange and transfer the certificate and private key to the server. When the user wishes to access a resource from the wireless device outside of the secure network demarcation line (102 in FIG. 3), they are prompted for a second means of authentication, which may be something the user has (such as</p>

Exhibit 730-Z
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Okereke

		<p>a swipe card, synchronized password keychain or channel key, for example), something the user is (such as a fingerprint scan), or something the user knows (such as a password or pass phrase). In a preferred embodiment this second form of authentication is something the user knows. The CPS verifies both forms of authentication, locates the user's certificate and establishes a session.” <i>Id.</i> at ¶32.</p>
1E	responsive to a determination that the scan data matches the biometric data,	<p>Okereke discloses responsive to a determination that the scan data matches the biometric data.</p> <p>For example, Okereke discloses taking action only if fingerprint is verified.</p> <p><i>See, e.g.,</i></p> <p>“As shown in FIG. 1, there is provided a traditional PKI system 10. The end user from the client workstation 20 sends a request 25 for a secure resource 50, and before access is granted, the user is requested 35 to provide a digital certificate 30 for authentication. The secure resource can be data, applications or other information of value. In some cases, once the digital certificate 30 is provided 40 and verified 55 by a certificate authority 60, access to the secure resource 50 will be granted as at 45. In other cases, an additional form of authentication may be required, such as a user name and password, a smart card, or a fingerprint, for example. The digital certificate verification process occurs through a certificate authority 60, normally a trusted third party.” <i>Id.</i> at ¶21.</p> <p>“In one embodiment of the invention, desktop software is used to authenticate the user to the CPS, register the wireless device with the CPS, facilitate the initial key exchange and transfer the certificate and private key to the server. When the user wishes to access a resource from the wireless device outside of the secure network demarcation line (102 in FIG. 3), they are prompted for a second means of authentication, which may be something the user has (such as a swipe card, synchronized password keychain or channel key, for example),</p>

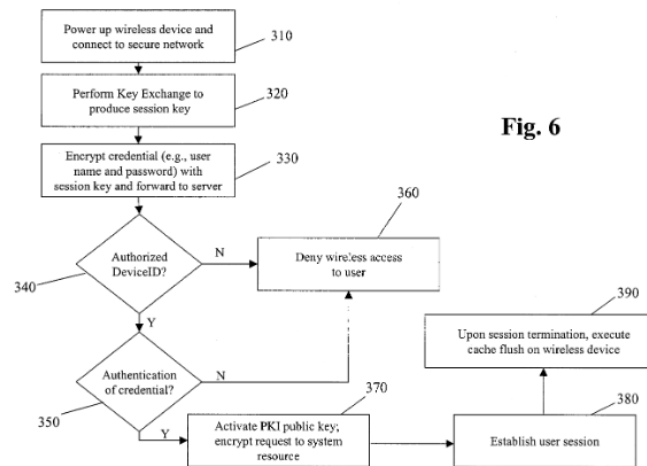
Exhibit 730-Z
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Okereke

		<p>something the user is (such as a fingerprint scan), or something the user knows (such as a password or pass phrase). In a preferred embodiment this second form of authentication is something the user knows. The CPS verifies both forms of authentication, locates the user's certificate and establishes a session.” <i>Id.</i> at ¶32.</p>
1F	<p>wirelessly sending one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values includes the device ID code; and</p>	<p>Okereke discloses wirelessly sending one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values includes the device ID code.</p> <p>For example, Okereke discloses wirelessly sending a unique identifier of a wireless device to a proxy server program for authorization, where the proxy server possess a list of unique identifiers belonging to devices that are registered with the server.</p> <p><i>See, e.g.,</i></p> <p style="text-align: right;">Fig. 4</p> <p><i>Id.</i> at Fig. 4.</p> <p>“The establishment of mobile access to secure resources in accordance with the present invention can occur as shown in FIGS. 4 and 5. The proxy server can be provided with software designed in accordance with the present invention, and a thin client application can be installed and/or downloaded onto the user's desktop computer. The proxy server program then awaits the initiation of a</p>

Exhibit 730-Z
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Okereke

request 210 from the desktop to establish secure wireless access capabilities using the system of the present invention. In so doing, a unique identifier for the wireless product to be employed is passed as at 210 to the proxy server 125 program for authorization. The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other device capable of remote wireless communication. The unique identifier can be a serial number or SIM. number, for example. If the unique identifier is one which the proxy server program identifies as being acceptable, the proxy server program will send approval as at 220 to the desktop 140, which executes functionality to make a key exchange as at 225, such as, for example, a Diffie Hellman Key Exchange.”

Id. at ¶25.



Id. at Fig. 6.

“If the user is authenticated by the proxy server matching the device unique identifier with authorized device identifications as at 340, and the credential information is authenticated as determined at 350, the proxy server will activate the user's PKI public key and request the secure network resource for the user, as at 370.”

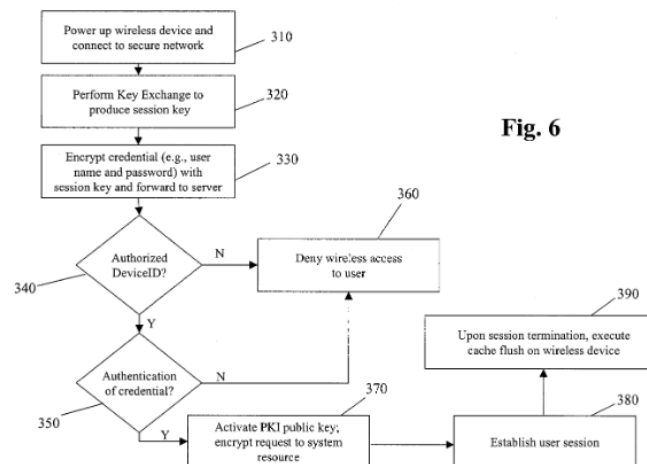
Exhibit 730-Z
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Okereke

		<p><i>Id.</i> at ¶28.</p> <p>“The user can ensure secure communication between the wireless device and the Certificate Proxy Server (CPS) in various ways, including physically connecting the device to the server, or connecting securely over a known trusted network. As the user's certificate and private key are securely transferred to the CPS, the unique network identifier for the user's wireless device (such as a SIM number) is registered with the server. This network identifier registration can also be done in a number of ways, including over the wireless network, or over a physical network.”</p> <p><i>Id.</i> at ¶30.</p>
1G	responsive to authentication of the one or more codes and the other data values by the agent,	<p>Okereke discloses responsive to authentication of the one or more codes and the other data values by the agent.</p> <p>For example, Okereke discloses taking action only if the users or the devices are authenticated by the proxy server.</p> <p><i>See, e.g.,</i></p> <p>Fig. 4</p> <p><i>Id.</i> at Fig. 4.</p> <p>“The establishment of mobile access to secure resources in accordance with the present invention can occur as shown in FIGS. 4 and 5. The proxy server can be provided with software designed in accordance with the present invention, and a thin client application can be installed and/or downloaded onto the user's</p>

Exhibit 730-Z
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Okereke

desktop computer. The proxy server program then awaits the initiation of a request 210 from the desktop to establish secure wireless access capabilities using the system of the present invention. In so doing, a unique identifier for the wireless product to be employed is passed as at 210 to the proxy server 125 program for authorization. The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other device capable of remote wireless communication. The unique identifier can be a serial number or SIM. number, for example. If the unique identifier is one which the proxy server program identifies as being acceptable, the proxy server program will send approval as at 220 to the desktop 140, which executes functionality to make a key exchange as at 225, such as, for example, a Diffie Hellman Key Exchange.”

Id. at ¶25.



Id. at Fig. 6.

“If the user is authenticated by the proxy server matching the device unique identifier with authorized device identifications as at 340, and the credential information is authenticated as determined at 350, the proxy server will activate

Exhibit 730-Z
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Okereke

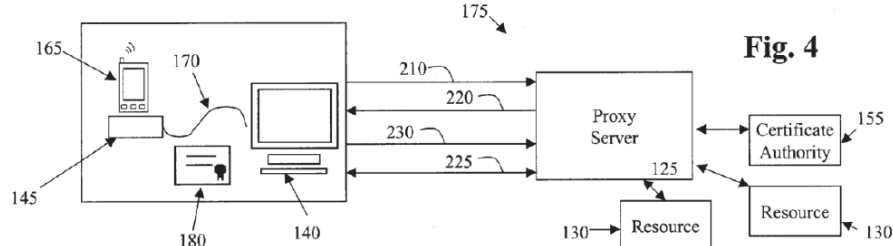
		<p>the user's PKI public key and request the secure network resource for the user, as at 370.” <i>Id.</i> at ¶28.</p> <p>“The user can ensure secure communication between the wireless device and the Certificate Proxy Server (CPS) in various ways, including physically connecting the device to the server, or connecting securely over a known trusted network. As the user's certificate and private key are securely transferred to the CPS, the unique network identifier for the user's wireless device (such as a SIM number) is registered with the server. This network identifier registration can also be done in a number of ways, including over the wireless network, or over a physical network.” <i>Id.</i> at ¶30.</p>
1H	receiving an access message from the agent allowing the user access to an application,	<p>Okereke discloses receiving an access message from the agent allowing the user access to an application.</p> <p>For example, Okereke discloses sending approval message from proxy server to devices and allow user session to begin after the devices and users are verified..</p> <p><i>See, e.g.,</i></p>  <p>Fig. 4</p> <p><i>Id.</i> at Fig. 4.</p> <p>“If the unique identifier is one which the proxy server program identifies as being acceptable, the proxy server program will send approval as at 220 to the</p>

Exhibit 730-Z
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Okereke

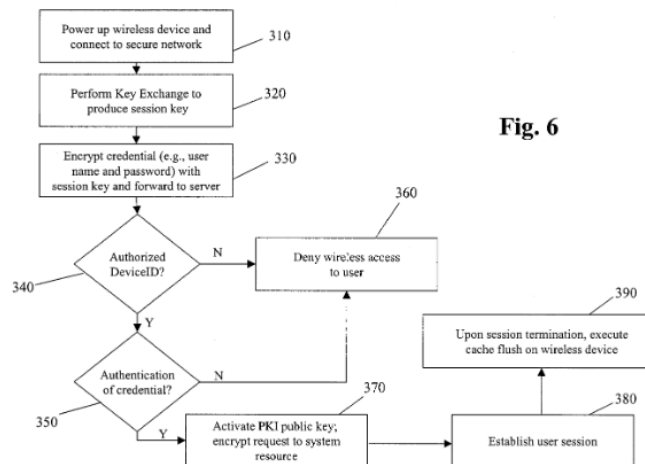
		<p>desktop 140, which executes functionality to make a key exchange as at 225, such as, for example, a Diffie Hellman Key Exchange.” <i>Id.</i> at ¶25.</p> <pre> graph TD 310[Power up wireless device and connect to secure network] --> 320[Perform Key Exchange to produce session key] 320 --> 330[Encrypt credential (e.g., user name and password) with session key and forward to server] 330 --> 340{Authorized DeviceID?} 340 -- N --> 360[Deny wire/less access to user] 340 -- Y --> 350{Authentication of credential?} 350 -- N --> 360 350 -- Y --> 370[Activate PKI public key; encrypt request to system resource] 370 --> 380[Establish user session] 380 --> 390[Upon session termination, execute cache flush on wireless device] </pre> <p align="center">Fig. 6</p> <p><i>Id.</i> at Fig. 6.</p> <p>“If the user is authenticated by the proxy server matching the device unique identifier with authorized device identifications as at 340, and the credential information is authenticated as determined at 350, the proxy server will activate the user's PKI public key and request the secure network resource for the user, as at 370. If the device identification is not authorized, or the user's credential is not authenticated, access to the user will be denied as at 360. The proxy server will then receive the request for digital certificate and private key, and provide the previously stored digital certificate and key, which can then be validated by the certificate authority, and the user's session can begin.” <i>Id.</i> at ¶28.</p>
1I	wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an	Okereke discloses wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

Exhibit 730-Z
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Okereke

ATM machine, a hard drive, computer software, a web site and a file.

For example, Okereke discloses that access would be given applications of either computer software, a file (or both).

See, e.g.,



Id. at Fig. 6.

“If the user is authenticated by the proxy server matching the device unique identifier with authorized device identifications as at 340, and the credential information is authenticated as determined at 350, the proxy server will activate the user's PKI public key and request the secure network resource for the user, as at 370. If the device identification is not authorized, or the user's credential is not authenticated, access to the user will be denied as at 360. The proxy server will then receive the request for digital certificate and private key, and provide the previously stored digital certificate and key, which can then be validated by the certificate authority, and the user's session can begin.”

Id. at ¶28.

Exhibit 730-Z
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Okereke

2	The method of claim 1, wherein the one or more codes and the other data values are transmitted to the agent over a network.	<p>Okereke discloses the one or more codes and the other data values are transmitted to the agent over a network</p> <p>For example, Okereke discloses transmitting device identifier over the Internet.</p> <p><i>See, e.g.,</i></p> <p>“In a specific embodiment as shown in FIG. 4, the user is first provided with a network-connected device, such as a desktop computer 140, along with one or more docking stations 145. One or more wireless-capable devices 165 may be docked in the docking station for two-way communication with the desktop computer as indicated at 170. The desktop computer includes a memory, processor, user interface, keyboard and mouse as is commonly known, and is preferably connected to a local area network (LAN) 175 for communication and use of shared resources as is commonly known.”</p> <p><i>Id.</i> at ¶24.</p> <p>“The proxy server can be provided with software designed in accordance with the present invention, and a thin client application can be installed and/or downloaded onto the user's desktop computer. The proxy server program then awaits the initiation of a request 210 from the desktop to establish secure wireless access capabilities using the system of the present invention. In so doing, a unique identifier for the wireless product to be employed is passed as at 210 to the proxy server 125 program for authorization. The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other device capable of remote wireless communication. The unique identifier can be a serial number or SIM. number, for example.”</p> <p><i>Id.</i> at ¶25.</p>
5	The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user.	<p>Okereke discloses the biometric data and the scan data are both based on a fingerprint scan by the user.</p> <p><i>See, e.g.,</i></p>

Exhibit 730-Z
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Okereke

		<p>“In other cases, an additional form of authentication may be required, such as a user name and password, a smart card, or a fingerprint, for example.” <i>Id.</i> at ¶21.</p> <p>“The credential information or authentication measure can be something the user has (such as a swipe card), something the user is (such as represented by a fingerprint scan), or something the user knows (such as a password or pass phrase)” <i>Id.</i> at ¶26.</p>
6	The method of claim 1, further comprising: establishing a secure communication channel prior to sending the one or more codes and the other data values for authentication.	<p>Okereke discloses establishing a secure communication channel prior to sending the one or more codes and the other data values for authentication.</p> <p>For example, Okereke discloses a security communication channel between device and proxy server.</p> <p><i>See,</i></p> <p>“The user can ensure secure communication between the wireless device and the Certificate Proxy Server (CPS) in various ways, including physically connecting the device to the server, or connecting securely over a known trusted network. As the user's certificate and private key are securely transferred to the CPS, the unique network identifier for the user's wireless device (such as a SIM number) is registered with the server. This network identifier registration can also be done in a number of ways, including over the wireless network, or over a physical network.” <i>Id.</i> at ¶30.</p>
8pre	An integrated device for verifying a user during authentication of the integrated device, comprising:	<p>Okereke discloses an integrated device for verifying a user during authentication of the integrated device.</p> <p><i>See</i> 1pre.</p>

Exhibit 730-Z
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Okereke

8A	a memory stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to the memory that is unable to be subsequently altered;	Okereke discloses a memory stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to the memory that is unable to be subsequently altered. <i>See 1A.</i>
8B	wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;	Okereke discloses wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition. <i>See 1B.</i>
8C	a verification unit, in communication with the memory, receives scan data from a biometric scan for comparison against the biometric data,	Okereke discloses a verification unit, in communication with the memory, receives scan data from a biometric scan for comparison against the biometric data, and if the scan data matches the biometric data. <i>See 1C-D.</i>
8D	and if the scan data matches the biometric data,	Okereke discloses if the scan data matches the biometric data. <i>See 1E.</i>
8E	wirelessly sends one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the	Okereke discloses wirelessly sends one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and the other data values includes the device ID code.

Exhibit 730-Z
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Okereke

	one or more codes and the other data values includes the device ID code; and	<i>See 1F.</i>
8F	responsive to the agent authenticating the one or more codes and the other data values,	Okereke discloses responsive to the agent authenticating the one or more codes and the other data values. <i>See 1G.</i>
8G	a radio frequency communicator, receives an access message from the agent allowing the user access to an application,	Okereke discloses a radio frequency communicator, receives an access message from the agent allowing the user access to an application. <i>See 1F, 1H.</i>
8H	wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.	Okereke discloses wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file. <i>See 1I.</i>
9	The integrated device of claim 8, wherein the one or more codes and the other data values are transmitted to the agent over a network.	Okereke discloses the one or more codes and the other data values are transmitted to the agent over a network. <i>See 2.</i>

Exhibit 905-X
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Johnson

US Patent No. 7,849,020 (“Johnson”) was filed March 15, 2006 and claims priority to April 19, 2005 and to the extend the ’905 Patent is found to not be entitled to priority date earlier than its application date, therefore qualifies as prior art under at least 35 U.S.C. §§ 102(a), (b), and (e) as to the asserted claims of U.S. Pat. No. 9,298,905 (“the ’905 Patent”). Johnson, including any material incorporated by reference into Johnson, anticipates claims 1, 4-5, 7, 9, 10, and 12 (“the Asserted Claims”) of the ’905 Patent under 35 U.S.C. § 102. Johnson also renders obvious the Asserted Claims under 35 U.S.C. § 103, alone based on the state of the art and/or in combination with one or more references identified in Samsung’s accompanying disclosure for the ’905 Patent.¹

To the extent Plaintiff alleges that Johnson does not disclose any particular limitation of the Asserted Claims of the ’905 Patent, either expressly or inherently, it would have been obvious to a person of ordinary skill in the art as of the priority date of the ’905 Patent to modify the Johnson reference and/or to combine the teachings of the Johnson reference with other prior art references, including but not limited to the present prior art references found in Exhibits 905-A-W and 905-Y-Z and the corresponding section(s) of charts for other prior art references for the ’905 Patent in a manner that would have rendered the Asserted Claims invalid as obvious.

With respect to the obviousness of the Asserted Claims under 35 U.S.C. § 103, one or more of the principles enumerated by the United States Supreme Court in *KSR v. Teleflex*, 550 U.S. 398 (2007) apply, including: (a) combining various claimed elements known in the prior art according to known methods to yield a predictable result; and/or (b) making a simple substitution of one or more known elements for another to obtain a predictable result; and/or (c) using a known technique to improve a similar device or method in the same way; and/or (d) applying a known technique to a known device or method ready for improvement to yield a predictable result; and/or (e) choosing from a finite number of identified, predictable solutions with a reasonable expectation of success or, in other words, the solution was one which was “obvious to try”; and/or (f) a known work in one field of endeavor prompting variations of it for use either in the same field or a different field based on given design incentives or other market forces in which the variations were predictable to one of ordinary skill in the art; and/or (g) a teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill in the art to modify the prior art reference or to combine the teachings of various prior art references to arrive at the claimed invention. It therefore would have been obvious to one of ordinary skill in the art to combine the disclosures of these references in accordance with the principles and rationales set forth above.

¹ Samsung notes that Plaintiff appears in many instances to be pursuing overly broad constructions of various limitations of the asserted claims of the ’905 Patent in an effort to piece together an infringement claim where none exists and to accuse a product that does not practice the claims. This claim chart may take into account Plaintiff’s overly broad constructions of the claim limitations. Any assertion that a particular limitation is disclosed by a prior art reference may be based on Plaintiff’s apparent constructions and is not intended to be, and is not, an admission that such constructions are supportable or proper.

Exhibit 905-X
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Johnson

The citations to portions of any reference in this chart are exemplary only. For example, a citation that refers to or discusses a figure or figure item should be understood to also incorporate by reference that figure and any additional descriptions of that figure as if set forth fully therein. Samsung reserves the right to rely on the entirety of the references cited in this chart to show that the Asserted Claims are invalid. Citations presented for one claim limitation are expressly incorporated by reference into all other limitations for that claim as well as all limitations of all claims on which that claim depends. Samsung also reserves the right to rely on additional citations or sources of evidence that also may be applicable, or that may become applicable in light of claim construction, changes in Plaintiff's infringement contentions, and/or information obtained during discovery as the case progresses.

Claim	U.S. Patent No. 9,298,905	Exemplary Disclosure in Johnson
1 pre	A method comprising:	The Preamble is not limiting.
1 A	persistently storing biometric data of a legitimate user and an ID code on an integrated device;	<p>Johnson renders obvious persistently storing biometric data of a legitimate user and an ID code on an integrated device.</p> <p>For example, Johnson discloses persistent storage of user specific information and tokens carrying device specific information such as a SIM number. While Johnson does not disclose the use of biometric data, it would be obvious to include.</p> <p><i>See, e.g.,</i></p> <p>“In one embodiment, various elements of an online transaction are distributed over separate and independent network entities. For example, the identity provider may provide identity validation in the form of an identity token, which the merchant can use to verify the identity of the purchaser. The identity token may include one or more identity credentials of the end-user. The identity token may be issued based on the identity information provided by the end-user/purchaser, for example, the subscribe number from the SIM card, a network address (e.g., a Network Interface Card (NIC) identification, World Wide Name (WWN), etc.), login information, etc. Similarly, the payment provider may provide verification of the end-user's ability to pay in the form of</p>

Exhibit 905-X
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Johnson

		<p>a payment token. In addition, the payment provider may handle payment transactions on behalf of the purchaser in satisfaction of the purchase of goods and/or services from the merchant. The above described framework allows, inter alia, a purchaser and merchant that are strangers to conduct an online commercial transaction in an untrusted network environment in relative confidence, as discussed in further detail in the various exemplary embodiments provided below.” <i>Id.</i> at 6:7-27.</p> <p>“To obtain an identity token, end-user 140 provides identity information to identity provider 120. Identity information may include any information that enables the identity provider 120 to distinguish between end-user utilizing end-user computer 110 and the various other end-users to which identity provider may provide services. For example, the identity information may include a unique identifier associated with the hardware of end-user computer 110. In one embodiment, the identity information is provided by a SIM card issuing an identifier unique to the subscriber. Identity information may include providing a unique hardware number of the network interface card (NIC) of the end-user computer 110, a world wide name (WWN) or other network address of end-user computer 110 or any other means by which end-user computer 110 may be identified, including (in some embodiments) an established login name/password combination.” <i>Id.</i> at 7:57-8:4.</p>
1B	responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;	<p>Johnson renders obvious responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor.</p> <p>For example, Johnson discloses user entry of a biometric sample for subsequent comparison. Although, Johnson does not disclose the use of biometrics it would be obvious to include it in this way.</p> <p><i>See, e.g.,</i></p>

Exhibit 905-X
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Johnson

		<p>“The identity provider 120 may transmit the identity token to end-user computer 110 to forward to merchant 140 (step 235), and/or identity provider 120 may transmit the identity token directly to the merchant 140. Merchant 140 may then process the identity token to identify end-user and/or to verify that end-user is who he/she purports to be. The identity token may be used to authenticate certain information about the end-user that may affect the transaction. For example, the merchant 140 may provide a service that requires the end-user to be of a certain age. Identity credentials transmitted with the identity token may be used to ensure that the end-user is of the proper age and meets this requirement. Merchant 140 may have discounts for particular end-users that are frequent purchasers, or who received a coupon, promotional offer, etc. The merchant 140 may index a database of end-users to determine whether the end-user qualifies or should otherwise be specially handled based on the provided identity credentials.</p> <p>Optionally, the merchant 140 may request validation of the identity token by sending a request to the identity provider 120 (step 245). The request for validation of the identity token may include forwarding the identity token from merchant 140 to identity provider 120. Upon receiving the request for validation of the identity token, the identity provider 120 may validate the identity token, and thereby determine whether the identity token is authentic. The identity provider 120 may then forward an indication of the validity of the identity token to the merchant 140 (step 255). Alternatively, the merchant 140 may simply validate the identity token itself (step 265) (e.g., by assuming the identity token is valid or otherwise processing the token). Optionally, a response may be returned from the merchant 140 to the end-user computer 110, where the response may include a message of whether the identity token is valid, of any applicable discount or promotional offers, and/or any other type of message, as the invention is not limited in this respect (step 265).” <i>Id.</i> at 8:46-9:14.</p>
--	--	--

Exhibit 905-X
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Johnson

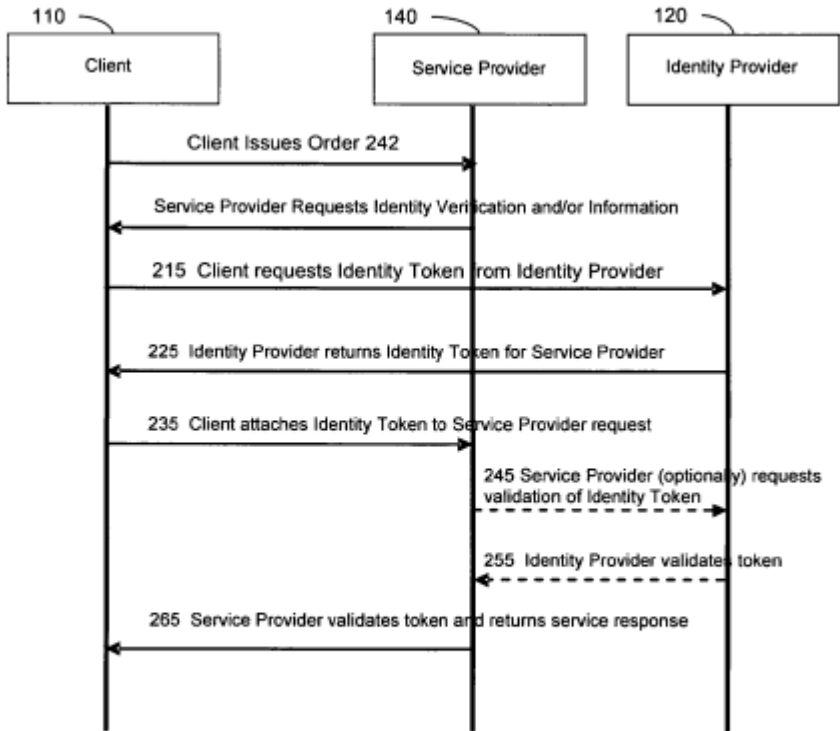
		 <pre> sequenceDiagram participant 110 as Client participant 140 as Service Provider participant 120 as Identity Provider 110->>140: Client Issues Order 242 140->>110: Service Provider Requests Identity Verification and/or Information 110->>120: 215 Client requests Identity Token from Identity Provider 120->>140: 225 Identity Provider returns Identity Token for Service Provider 110->>140: 235 Client attaches Identity Token to Service Provider request 140->>120: 245 Service Provider (optional) requests validation of Identity Token 120->>140: 255 Identity Provider validates token 140->>110: 265 Service Provider validates token and returns service response </pre> <p align="center">FIG. 2</p>
1C	<p>comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;</p>	<p>Johnson renders obvious comparing the scan data to the biometric data to determine whether the scan data matches the biometric data.</p> <p>Although, Johnson does not disclose the use of biometrics it would be obvious to include it in this way.</p>

Exhibit 905-X
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Johnson

		<p><i>See, e.g.,</i></p> <p>“The identity provider 120 may transmit the identity token to end-user computer 110 to forward to merchant 140 (step 235), and/or identity provider 120 may transmit the identity token directly to the merchant 140. Merchant 140 may then process the identity token to identify end-user and/or to verify that end-user is who he/she purports to be. The identity token may be used to authenticate certain information about the end-user that may affect the transaction. For example, the merchant 140 may provide a service that requires the end-user to be of a certain age. Identity credentials transmitted with the identity token may be used to ensure that the end-user is of the proper age and meets this requirement. Merchant 140 may have discounts for particular end-users that are frequent purchasers, or who received a coupon, promotional offer, etc. The merchant 140 may index a database of end-users to determine whether the end-user qualifies or should otherwise be specially handled based on the provided identity credentials.</p> <p>Optionally, the merchant 140 may request validation of the identity token by sending a request to the identity provider 120 (step 245). The request for validation of the identity token may include forwarding the identity token from merchant 140 to identity provider 120. Upon receiving the request for validation of the identity token, the identity provider 120 may validate the identity token, and thereby determine whether the identity token is authentic. The identity provider 120 may then forward an indication of the validity of the identity token to the merchant 140 (step 255). Alternatively, the merchant 140 may simply validate the identity token itself (step 265) (e.g., by assuming the identity token is valid or otherwise processing the token). Optionally, a response may be returned from the merchant 140 to the end-user computer 110, where the response may include a message of whether the identity token is valid, of any applicable discount or promotional offers, and/or any other type of message, as the invention is not limited in this respect (step 265).” <i>Id.</i> at 8:46-9:14.</p>
--	--	---

Exhibit 905-X
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Johnson

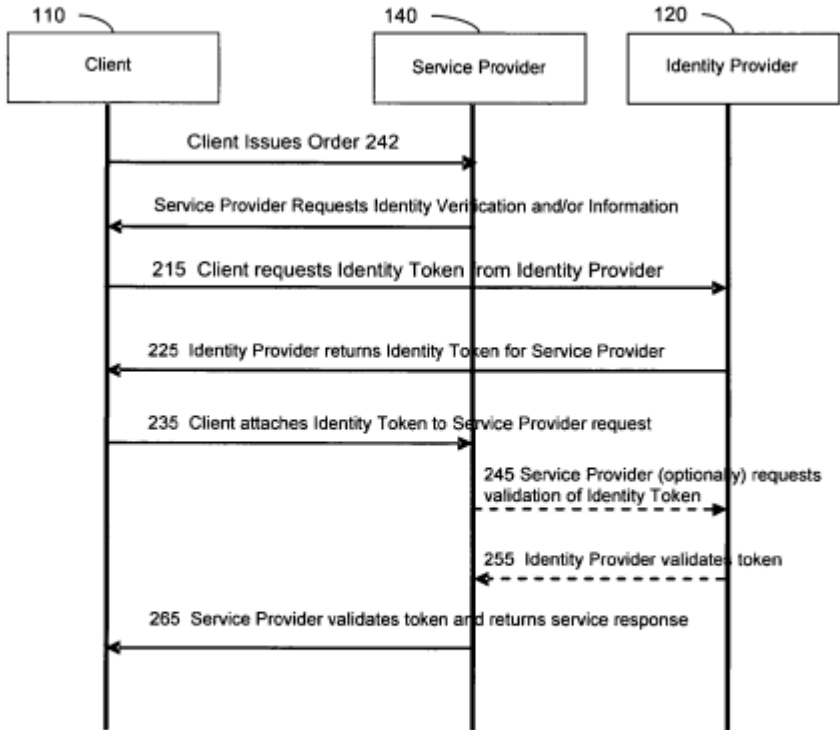
		 <pre> sequenceDiagram participant 110 as Client participant 140 as Service Provider participant 120 as Identity Provider 110->>140: Client Issues Order 242 140->>110: Service Provider Requests Identity Verification and/or Information 110->>120: 215 Client requests Identity Token from Identity Provider 120->>140: 225 Identity Provider returns Identity Token for Service Provider 110->>140: 235 Client attaches Identity Token to Service Provider request 140->>120: 245 Service Provider (optional) requests validation of Identity Token 120->>140: 255 Identity Provider validates token 140->>110: 265 Service Provider validates token and returns service response </pre> <p align="center">FIG. 2</p>
1D	responsive to a determination that the scan data matches the biometric data,	Johnson renders obvious responsive to a determination that the scan data matches the biometric data.

Exhibit 905-X
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Johnson

		<p>For example, Johnson discloses appropriately sending an identity token during a requested transaction. Although, Johnson does not disclose the use of biometrics it would be obvious to include it in this way.</p> <p><i>See, e.g.,</i></p> <p>“The identity provider 120 may transmit the identity token to end-user computer 110 to forward to merchant 140 (step 235), and/or identity provider 120 may transmit the identity token directly to the merchant 140. Merchant 140 may then process the identity token to identify end-user and/or to verify that end-user is who he/she purports to be. The identity token may be used to authenticate certain information about the end-user that may affect the transaction. For example, the merchant 140 may provide a service that requires the end-user to be of a certain age. Identity credentials transmitted with the identity token may be used to ensure that the end-user is of the proper age and meets this requirement. Merchant 140 may have discounts for particular end-users that are frequent purchasers, or who received a coupon, promotional offer, etc. The merchant 140 may index a database of end-users to determine whether the end-user qualifies or should otherwise be specially handled based on the provided identity credentials.</p> <p>Optionally, the merchant 140 may request validation of the identity token by sending a request to the identity provider 120 (step 245). The request for validation of the identity token may include forwarding the identity token from merchant 140 to identity provider 120. Upon receiving the request for validation of the identity token, the identity provider 120 may validate the identity token, and thereby determine whether the identity token is authentic. The identity provider 120 may then forward an indication of the validity of the identity token to the merchant 140 (step 255). Alternatively, the merchant 140 may simply validate the identity token itself (step 265) (e.g., by assuming the identity token is valid or otherwise processing the token).</p> <p>Optionally, a response may be returned from the merchant 140 to the end-user computer 110, where the response may include a message of whether the identity token is valid, of any applicable discount or promotional offers, and/or</p>
--	--	---

Exhibit 905-X
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Johnson

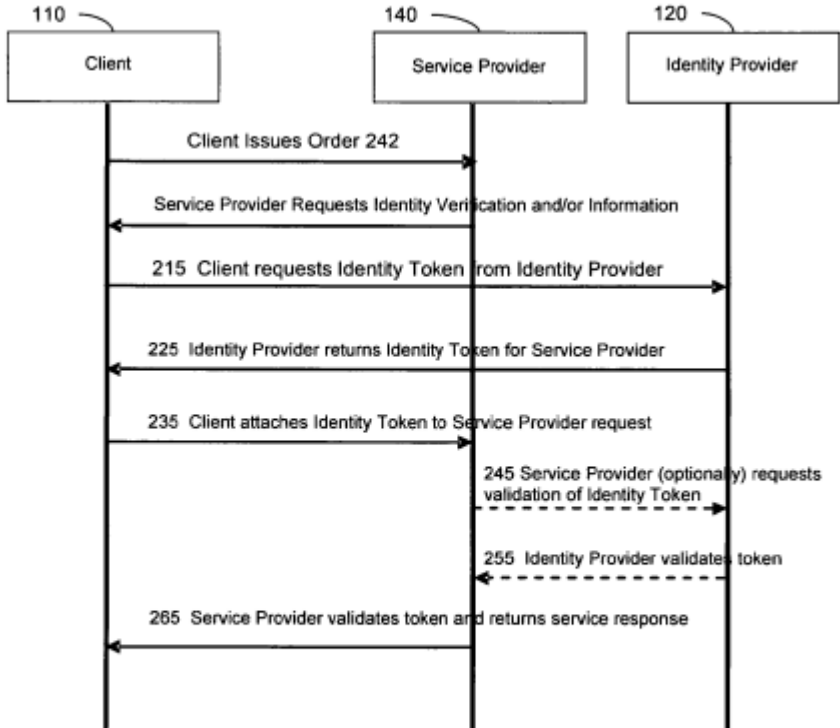
		<p>any other type of message, as the invention is not limited in this respect (step 265).” <i>Id.</i> at 8:46-9:14.</p>  <pre> sequenceDiagram participant 110 as Client participant 140 as Service Provider participant 120 as Identity Provider 110->>140: Client Issues Order 242 140->>110: Service Provider Requests Identity Verification and/or Information 110->>120: 215 Client requests Identity Token from Identity Provider 120->>140: 225 Identity Provider returns Identity Token for Service Provider 110->>140: 235 Client attaches Identity Token to Service Provider request 140->>120: 245 Service Provider (optional) requests validation of Identity Token 120->>140: 255 Identity Provider validates token 140->>110: 265 Service Provider validates token and returns service response </pre> <p align="center">FIG. 2</p>
1E	wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously	Johnson discloses wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority.

Exhibit 905-X
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Johnson

	<p>registered ID codes maintained by the third-party trusted authority; and</p>	<p>For example, Johnson discloses sending device IDs and other information and codes to a central database for verification.</p> <p><i>See, e.g.,</i></p> <p>“An end-user computer 110 may place an order 242 with a merchant 140. The order 242 may be any indication that the end-user would like to purchase one or more goods and/or services from the merchant 140. For example, the order 242 may result from end-user selecting a good or service via a web browser displaying pages resident at the website of a merchant, or may result from choosing an option from an application running locally, as described in further detail below. As an example of the first instance, the merchant 140 may provide a website to display or otherwise offer for sale goods and/or services that it provides, or may provide an online catalog of merchandise. The order 242 may be any type of indication that end-user would like to purchase one or more goods and/or services from the merchant 140.</p> <p>As an example of the second instance and as an alternative to selecting one or more goods and services from a merchant's website, order 242 may originate from an application or other program local to the end-user computer 110. For example, an end user may create, produce or edit a document via a word processing application, design a slide show using a presentation application and/or manipulate images or graphics for a poster or brochure using an imaging application. The application may include an option under the print menu that allows the document to be printed by a third party to, for example, take advantage of printing features that may not be locally available, or to otherwise exploit professional printing services. When the option is selected, the application may send, via the network, order 242 to the merchant 140. It should be appreciated that order 242 may be any indication to purchase any good and/or service, as the aspects of the invention are not limited in this respect.</p> <p>In response to order 242, merchant 140 may request that end-user 110 provide an indication of the end-user's identity and/or verification that the end-user is</p>
--	---	--

Exhibit 905-X
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Johnson

		<p>indeed who he/she purports to be (step 205). For example, merchant 140 may not know anything about the source of order 242 and may desire information about the identity of the end-user and/or assurance that the end-user is not spoofing his/her identity. Alternatively, the merchant 140 may send a notice or indication that payment is required for the service and demand that a payment token be provided. To obtain a payment token, it may be necessary to first establish an identity via an identity token, as described in further detail below. In either case, end-user 110 may respond to the request by the merchant 140 by enlisting the services of identity provider 120 (step 215).” <i>Id.</i> 7:11-7:55.</p> <p>“From the perspective of the merchant, the commercial transaction is substantially risk free as the identity of the end-user and the payment verification is handled by third parties and is therefore less susceptible to fraud, spoofing and even innocent mistakes in providing personal and financial information. Therefore, merchants may be more willing to conduct online commercial transactions with unknown end-users over an untrusted network. From the perspective of the end-user, personal and financial information resides with entities either that already maintain the information and/or that the end-user has an established relationship with. Confidential personal and financial end-user information need not be provided to the merchant, mitigating the vulnerabilities of having confidential information misused or misappropriated. As a result, end-users may be more willing to conduct commercial transactions with unknown merchants without having to worry about whether the merchant is trustworthy or not.</p> <p>In some conventional commercial transaction models, identity information and payment information are input by the user and processed by either a third party or the merchant. As discussed above, these models are awkward, inefficient and time consuming for the user. In addition, conventional models present numerous issues regarding security of an end-user's confidential information as well as making a merchant vulnerable to fraud and/or susceptible to failure to pay by an end-user. Applicant has appreciated that commercial transaction software installed on each of the computers employed in various commercial</p>
--	--	--

Exhibit 905-X
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Johnson

		<p>transactions may mitigate or eliminate concerns over security and fraud. In addition, many of the actions handled by the end-user and merchant in conventional models may be performed by the commercial transactions software, making the transaction simpler and more intuitive to the end-user.” <i>Id.</i> at 10:47-11:12.</p>
1F	<p>responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code,</p>	<p>Johnson discloses responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code.</p> <p>For example, Johnson discloses returning results of verification process to the local device and user and transmitting an authentication output following verification of biometric data.</p> <p><i>See, e.g.,</i></p> <p>“The identity provider 120 may transmit the identity token to end-user computer 110 to forward to merchant 140 (step 235), and/or identity provider 120 may transmit the identity token directly to the merchant 140. Merchant 140 may then process the identity token to identify end-user and/or to verify that end-user is who he/she purports to be. The identity token may be used to authenticate certain information about the end-user that may affect the transaction. For example, the merchant 140 may provide a service that requires the end-user to be of a certain age. Identity credentials transmitted with the identity token may be used to ensure that the end-user is of the proper age and meets this requirement. Merchant 140 may have discounts for particular end-users that are frequent purchasers, or who received a coupon, promotional offer, etc. The merchant 140 may index a database of end-users to determine whether the end-user qualifies or should otherwise be specially handled based on the provided identity credentials.</p> <p>Optionally, the merchant 140 may request validation of the identity token by sending a request to the identity provider 120 (step 245). The request for</p>

Exhibit 905-X
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Johnson

		<p>validation of the identity token may include forwarding the identity token from merchant 140 to identity provider 120. Upon receiving the request for validation of the identity token, the identity provider 120 may validate the identity token, and thereby determine whether the identity token is authentic. The identity provider 120 may then forward an indication of the validity of the identity token to the merchant 140 (step 255). Alternatively, the merchant 140 may simply validate the identity token itself (step 265) (e.g., by assuming the identity token is valid or otherwise processing the token). Optionally, a response may be returned from the merchant 140 to the end-user computer 110, where the response may include a message of whether the identity token is valid, of any applicable discount or promotional offers, and/or any other type of message, as the invention is not limited in this respect (step 265).</p> <p>After the merchant 140 has processed the identity token and/or has received a validation for the identity token from the identity provider 120, the merchant 140 may request that the end-user provide verification or validation of an ability to pay and/or provide an indication of how the end-user would like to pay for the goods or services. The merchant 140 may make the request via a payment token request (step 305 in FIG. 3). In response to the payment token request, the end-user computer 110 may enlist the services of a payment provider 130. Payment provider 130 may be associated with a third party that maintains financial and payment information about various end-users, such as a financial institution, or a third party broker that handles financial transactions and payment procedures.</p> <p>The end-user computer 110 may solicit a payment token from a payment provider 130 (step 315) by transmitting the identity token to payment provider 130. Alternatively, the end-user may request a payment token by logging onto the payment provider 130 in a manner similar to that discussed in connection with the identity provider 120 (i.e., by providing an identifier such as a SIM subscriber number, NIC address and/or using a login/password combination). It should be appreciated that the end-user may request a payment token in other ways, as the invention is not limited in this respect. In addition, the end-user may send information about the purchase, such as the price and</p>
--	--	---

Exhibit 905-X
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Johnson

		<p>nature of the purchase so that the payment provider can verify that the end-user is capable of paying. However, providing purchase information is not required, as it may not be necessary or it may be handled in subsequent steps of the transaction.” <i>Id.</i> at 8:46-9:44</p> <p>“In one embodiment, the local installation of the commercial transaction software 485 a on identity provider 420 can create an identity token identifying the end-user utilizing end-user computer 410. Furthermore, the commercial transaction software 485 a on identity provider 420 can forward the identity token to the end-user computer 410, the payment provider 430, the merchant 440, and/or any other computer, as the invention is not limited in this respect. The local installation of the commercial transaction software 485 b on the end-user computer 410 can issue identity information (so as to identify the end-user) in response to an indication to conduct an online transaction between the end-user and a merchant. The local installation of the commercial transaction software 485 c installed on payment provider 430 can receive the identity token and generate a payment token verifying an ability of the end-user to pay (e.g., the payment token) for the online transaction. The local installation of the commercial transaction software 485 d installed on the merchant 440 can receive the verification of the ability of the end-user to pay before proceeding with the online transaction.</p> <p>In one embodiment, each of the computers in system 400 operates using a local installation of a same or similar operating system 495. For example, each of the computers in system 400 may operate using the Microsoft Windows® operating system. Commercial transactions software 485 may be a subsystem of the operating system. In this way, the various computers employed in a commercial transaction communicate in a consistent and known fashion. Since the commercial transactions software is communicating directly over the network and handling the validation, verification and security, the end-user and merchant need not know anything about one another, and more importantly, may not need to establish any trust relationship. In addition, because certain portions of the transactions are handled by the operating system, much of the</p>
--	--	---

Exhibit 905-X
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Johnson

		<p>transaction may be performed substantially invisible to the user, without requiring confusing and often times awkward involvement by the end-user. By having the commercial transactions software on each computer, various encryption techniques may be used during transmission of information from one computer to another. Moreover, further security features may be included such as identity tokens and/or payment tokens that are valid for a limited time period. For example, an identity token may include a time component that specifies a time after which any component receiving and processing the token should deem it invalid, and not honor the token as verification of identity and/or payment. The commercial transactions software components may programmatically process any time limits associated with a token. This may prevent tokens obtained by “fishing” from being used inappropriately at a later date.” <i>Id.</i> at 11:34-12:16</p>
1G	allowing the user to complete a financial transaction.	<p>Johnson discloses allowing the user to complete a financial transaction.</p> <p>For example, Johnson discloses the system can be used in an online financial transaction process.</p> <p><i>See, e.g.,</i></p> <p>“Conventional models for networked commercial transactions focus on the browser as the interface for requesting and submitting personal and financial information between an end-user purchaser and a merchant or service provider, whether it be directly through the merchant or via a third party transaction provider. In the first instance, the merchant is burdened with creating and maintaining an infrastructure capable of querying, obtaining, handling and processing personal and financial information, typically with some minimum level of security. Moreover, the merchant may be responsible for maintaining accounts and account information for each of its customers (which typically includes both confidential personal and financial information).” <i>Id.</i> at 4:8-21.</p>

Exhibit 905-X
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Johnson

		<p>“Conventional online transactions, for example, the purchase of goods and/or services over a network, are vulnerable to security breaches resulting in loss of personal, financial and/or other confidential information. Moreover, in an untrusted network (e.g., the Internet), both merchants and purchasers are at risk for entering into a transaction with a bad actor such that one side of the bargain is not upheld. Conventional online transaction models may also require a merchant to archive purchaser's confidential information and may require them to handle payment aspects of the transaction. In addition, conventional online transaction models are awkward for the purchaser and produce a generally unintuitive transaction experience. For example, conventional online transactions are conducted via a browser using a login/password paradigm that is confusing and difficult to manage.</p> <p>Applicant has identified and appreciated that delegating at least some of the transactional responsibilities handled by the purchaser and browser in conventional models to lower level systems (and away from the browser and end-user), may facilitate a simpler and more secure online commercial transactions framework. For example, one or more transactional tasks may be handled by the operating system at one or both of the end-user and merchant, where information may be more securely safeguarded. By embedding one or more tasks in the operating system, users may be relieved of some of the burden of transferring transactional information, making the experience more intuitive and enhancing security. Moreover, the merchant may be relieved of maintaining purchaser information, handling of payment information and/or processing the transaction.” <i>Id.</i> at 3:22-52.</p>
4	The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.	<p>Johnson renders obvious wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.</p> <p>Although, Johnson does not disclose the use of biometrics it would be obvious to include it in this way.</p>

Exhibit 905-X
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Johnson

		<p><i>See, e.g.,</i></p> <p>“The identity provider 120 may transmit the identity token to end-user computer 110 to forward to merchant 140 (step 235), and/or identity provider 120 may transmit the identity token directly to the merchant 140. Merchant 140 may then process the identity token to identify end-user and/or to verify that end-user is who he/she purports to be. The identity token may be used to authenticate certain information about the end-user that may affect the transaction. For example, the merchant 140 may provide a service that requires the end-user to be of a certain age. Identity credentials transmitted with the identity token may be used to ensure that the end-user is of the proper age and meets this requirement. Merchant 140 may have discounts for particular end-users that are frequent purchasers, or who received a coupon, promotional offer, etc. The merchant 140 may index a database of end-users to determine whether the end-user qualifies or should otherwise be specially handled based on the provided identity credentials.</p> <p>Optionally, the merchant 140 may request validation of the identity token by sending a request to the identity provider 120 (step 245). The request for validation of the identity token may include forwarding the identity token from merchant 140 to identity provider 120. Upon receiving the request for validation of the identity token, the identity provider 120 may validate the identity token, and thereby determine whether the identity token is authentic. The identity provider 120 may then forward an indication of the validity of the identity token to the merchant 140 (step 255). Alternatively, the merchant 140 may simply validate the identity token itself (step 265) (e.g., by assuming the identity token is valid or otherwise processing the token).</p> <p>Optionally, a response may be returned from the merchant 140 to the end-user computer 110, where the response may include a message of whether the identity token is valid, of any applicable discount or promotional offers, and/or any other type of message, as the invention is not limited in this respect (step 265).” <i>Id.</i> at 8:46-9:14.</p>
--	--	--

Exhibit 905-X
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Johnson

		<pre> sequenceDiagram participant 110 as Client participant 140 as Service Provider participant 120 as Identity Provider 110->>140: Client Issues Order 242 140->>110: Service Provider Requests Identity Verification and/or Information 110->>120: 215 Client requests Identity Token from Identity Provider 120->>110: 225 Identity Provider returns Identity Token for Service Provider 110->>140: 235 Client attaches Identity Token to Service Provider request 140->>120: 245 Service Provider (optional) requests validation of Identity Token 120->>140: 255 Identity Provider validates token 140->>110: 265 Service Provider validates token and returns service response </pre> <p align="center">FIG. 2</p>
5	<p>The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.</p>	<p>Johnson discloses wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.</p>

Exhibit 905-X
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Johnson

		<p>For example, Johnson discloses personal digital assistant (PDA) and cellular telephone.</p> <p><i>See, e.g.,</i> “The proliferation of networked computer systems has opened up new possibilities with respect to how corporations and individuals conduct business. For example, end-users connected to a network, (e.g., the Internet), via a networked device such as a computer, PDA, cellular phone, etc., may conduct commercial transactions over the network to purchase services and/or merchandise, conduct financial transactions, or otherwise conduct business or perform personal transactions over the network.” <i>Id.</i> at 1:19-27.</p>
7	<p>The method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.</p>	<p>Johnson discloses wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.</p> <p>For example, Johnson discloses use of the system with an ATM, computer, and vending machine.</p> <p><i>See, e.g.,</i> “The end-user computer 110 may solicit a payment token from a payment provider 130 (step 315) by transmitting the identity token to payment provider 130. Alternatively, the end-user may request a payment token by logging onto the payment provider 130 in a manner similar to that discussed in connection with the identity provider 120 (i.e., by providing an identifier such as a SIM subscriber number, NIC address and/or using a login/password combination). It should be appreciated that the end-user may request a payment token in other ways, as the invention is not limited in this respect. In addition, the end-user may send information about the purchase, such as the price and nature of the purchase so that the payment provider can verify that the end-user is capable of paying. However, providing purchase information is not required,</p>

Exhibit 905-X
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Johnson

		<p>as it may not be necessary or it may be handled in subsequent steps of the transaction.” <i>Id.</i> at 9:29-44</p> <p>“In one embodiment, each of the computers in system 400 operates using a local installation of a same or similar operating system 495. For example, each of the computers in system 400 may operate using the Microsoft Windows® operating system. Commercial transactions software 485 may be a subsystem of the operating system. In this way, the various computers employed in a commercial transaction communicate in a consistent and known fashion. Since the commercial transactions software is communicating directly over the network and handling the validation, verification and security, the end-user and merchant need not know anything about one another, and more importantly, may not need to establish any trust relationship. In addition, because certain portions of the transactions are handled by the operating system, much of the transaction may be performed substantially invisible to the user, without requiring confusing and often times awkward involvement by the end-user. By having the commercial transactions software on each computer, various encryption techniques may be used during transmission of information from one computer to another. Moreover, further security features may be included such as identity tokens and/or payment tokens that are valid for a limited time period. For example, an identity token may include a time component that specifies a time after which any component receiving and processing the token should deem it invalid, and not honor the token as verification of identity and/or payment. The commercial transactions software components may programmatically process any time limits associated with a token. This may prevent tokens obtained by “fishing” from being used inappropriately at a later date.” <i>Id.</i> at 11:54-12:16</p> <p><i>See also</i> 1G.</p>
9pre	An integrated device comprising:	<p>Johnson discloses an integrated device.</p> <p><i>See</i> 1pre.</p>

Exhibit 905-X
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Johnson

9A	a persistent storage media that persistently stores biometric data of a user and an ID code;	Johnson discloses a persistent storage media that persistently stores biometric data of a user and an ID code. <i>See</i> IA.
9B	a validation module, coupled to communicate with the persistent storage media,	Johnson discloses a validation module, coupled to communicate with the persistent storage media, <i>See</i> 1B-1C.
9C	that receives scan data from a biometric scan for comparison against the biometric data,	Johnson discloses receiving scan data from a biometric scan for comparison against the biometric data. <i>See</i> 1B-1C.
9D	and that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and	Johnson discloses sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority. <i>See</i> 1E.
9E	a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and	Johnson discloses a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third-party trusted authority Successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to-complete a financial transaction. <i>See</i> 1E.
9F	allowing the user to-complete a financial transaction.	Johnson discloses allowing the user to-complete a financial transaction. <i>See</i> 1F

Exhibit 905-X
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Johnson

10	The integrated device of claim 7, wherein the ID code is transmitted to the third-party trusted authority over a network.	<p>Johnson discloses wherein the ID code is transmitted to the third-party trusted authority over a network.</p> <p>For example, Johnson discloses communication for verification over the Internet.</p> <p>“Network 105 may be any type of network in any type of configuration that interconnects and allows nodes connected to the network to communicate. Nodes or devices may be connected to the network via copper (e.g., Category 5) cable, optical connections, wireless or any combination thereof. Information may be transferred using any low level protocol such as Ethernet and/or any information protocol such as TCP/IP. The network 105 may have any number of devices connected to it and may be a trusted (e.g., intranet) or an untrusted network (e.g., LAN/WAN, Internet, etc.), or a combination of both. The computers connected to the network may be any type of device including, but not limited to, one or any combination of a mobile phone, a desktop computer, a tablet personal computer, a server, workstation, etc.” <i>Id.</i> at 6:47-60.</p>
12	The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.	<p>Johnson discloses the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.</p> <p><i>See 5.</i></p>

Exhibit 905-Y
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Ludtke

US Patent No. 7,188,110 (“Ludtke”) was filed on December 11, 2000 and issued on March 6, 2007, and therefore qualifies as prior art under at least 35 U.S.C. §§ 102(a), (b), and (e) as to the asserted claims of U.S. Pat. No. 9,298,905 (“the ’905 Patent”). Ludtke, including any material incorporated by reference into Ludtke, anticipates claims 1, 4-5, 7, 9, 10, and 12 (“the Asserted Claims”) of the ’905 Patent under 35 U.S.C. § 102. Ludtke also renders obvious the Asserted Claims under 35 U.S.C. § 103, alone based on the state of the art and/or in combination with one or more references identified in Samsung’s accompanying disclosure for the ’905 Patent.¹

To the extent Plaintiff alleges that Ludtke does not disclose any particular limitation of the Asserted Claims of the ’905 Patent, either expressly or inherently, it would have been obvious to a person of ordinary skill in the art as of the priority date of the ’905 Patent to modify the Ludtke reference and/or to combine the teachings of the Ludtke reference with other prior art references, including but not limited to the present prior art references found in Exhibits 905-A-X and 905-Z and the corresponding section(s) of charts for other prior art references for the ’905 Patent in a manner that would have rendered the Asserted Claims invalid as obvious.

With respect to the obviousness of the Asserted Claims under 35 U.S.C. § 103, one or more of the principles enumerated by the United States Supreme Court in *KSR v. Teleflex*, 550 U.S. 398 (2007) apply, including: (a) combining various claimed elements known in the prior art according to known methods to yield a predictable result; and/or (b) making a simple substitution of one or more known elements for another to obtain a predictable result; and/or (c) using a known technique to improve a similar device or method in the same way; and/or (d) applying a known technique to a known device or method ready for improvement to yield a predictable result; and/or (e) choosing from a finite number of identified, predictable solutions with a reasonable expectation of success or, in other words, the solution was one which was “obvious to try”; and/or (f) a known work in one field of endeavor prompting variations of it for use either in the same field or a different field based on given design incentives or other market forces in which the variations were predictable to one of ordinary skill in the art; and/or (g) a teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill in the art to modify the prior art reference or to combine the teachings of various prior art references to arrive at the claimed invention. It therefore would have been obvious to one of ordinary skill in the art to combine the disclosures of these references in accordance with the principles and rationales set forth above.

The citations to portions of any reference in this chart are exemplary only. For example, a citation that refers to or discusses a figure or figure item should be understood to also incorporate by reference that figure and any additional descriptions of that figure as if set

¹ Samsung notes that Plaintiff appears in many instances to be pursuing overly broad constructions of various limitations of the asserted claims of the ’905 Patent in an effort to piece together an infringement claim where none exists and to accuse a product that does not practice the claims. This claim chart may take into account Plaintiff’s overly broad constructions of the claim limitations. Any assertion that a particular limitation is disclosed by a prior art reference may be based on Plaintiff’s apparent constructions and is not intended to be, and is not, an admission that such constructions are supportable or proper.

Exhibit 905-Y
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Ludtke

forth fully therein. Samsung reserves the right to rely on the entirety of the references cited in this chart to show that the Asserted Claims are invalid. Citations presented for one claim limitation are expressly incorporated by reference into all other limitations for that claim as well as all limitations of all claims on which that claim depends. Samsung also reserves the right to rely on additional citations or sources of evidence that also may be applicable, or that may become applicable in light of claim construction, changes in Plaintiff's infringement contentions, and/or information obtained during discovery as the case progresses.

Claim	U.S. Patent No. 9,298,905	Exemplary Disclosure in Ludtke
1pre	A method comprising:	The Preamble is not limiting.
1A	persistently storing biometric data of a legitimate user and an ID code on an integrated device;	<p>Ludtke discloses persistently storing biometric data of a legitimate user and an ID code on an integrated device.</p> <p>For example, Ludtke discloses using transaction device information as ID code and storing fingerprint data on the integrated transaction device.</p> <p><i>See, e.g.,</i></p> <p>“The fingerprint data entry process may be performed at least twice, to confirm that the user has entered the correct data (using the correct fingerprint). If confirmation succeeds, the device writes the fingerprint image data into write-once memory, or other memory that is protected from accidental modification.” Ludtke at 19:35-40.</p> <p>“The privacy card records the keys in its own permanent, secure memory. Thereafter, subsequent access to the privacy card by the user requires secure exchange between the card and digital wallet.” <i>Id.</i> at 21:46-50</p> <p>“One embodiment of a system is illustrated in FIG. 1. In this embodiment, a transaction privacy clearing house (TPCH) 110 interfaces a user 120 and a vendor 125. In this particular embodiment, a transaction device, e.g., a privacy card 130, is used to maintain the privacy of the user while enabling the user to</p>

Exhibit 905-Y
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Ludtke

		<p>perform transactions. The transaction device information is provided to the TPCCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed.</p> <p>In order to maintain confidentiality of the identity of the user, the transaction device information does not provide user identification information. Thus, the vendor or other entities do not have user information but rather transaction device information. The TPCCH 110 maintains a secure database of transaction device information and user information.”</p> <p><i>Id.</i> at 6:36-51.</p>
1B	responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;	<p>Ludtke discloses responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor.</p> <p>For example, Ludtke discloses using biometric verification through a biometric sensor – including a fingerprint through a fingerprint sensor– to verify the user of the device.</p> <p><i>See, e.g.,</i></p>

Exhibit 905-Y
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Ludtke

		<div data-bbox="932 211 1558 824" data-label="Diagram"> </div> <p style="text-align: center;">FIG. 28</p> <p><i>Id.</i> at Fig. 28.</p> <p>“FIG. 28 illustrates one embodiment of a device, as a consumer access device, 2802 that implements the method discussed above. The consumer access device 2802 has an LCD screen 2804 showing text, a biometric identification unit, in this embodiment as a Fingerprint Identification Unit (FIU) 2806 and a touchpad 2808 for user input. The user of the consumer access device 2802 would be authorized access to the device 2802 if the device recognized the user after the user had pressed his finger against the FIU 2806.”</p> <p><i>Id.</i> at 39:19-27.</p>
--	--	--

Exhibit 905-Y
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Ludtke

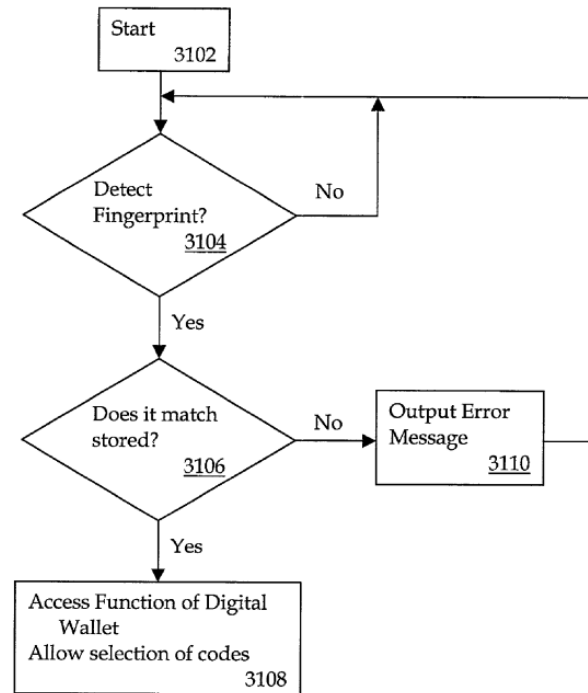


FIG. 31

Id. at Fig. 31.

“FIG. 31 illustrates one embodiment of a method to securely and conveniently store and transmit telephony-based data. At 3102 the user may start a device, such as a digital wallet (DW). At 3104 the DW checks to see if a fingerprint has been detected. If not then the DW loops back looking for a fingerprint. If a fingerprint has been detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint. If a match does not occur, then at 3110 an error message is output and the DW returns to checking to see if a fingerprint has been detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes.”

Exhibit 905-Y
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Ludtke

		<i>Id.</i> at 39:47-59.
1C	comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;	<p>Ludtke discloses comparing the scan data to the biometric data to determine whether the scan data matches the biometric data.</p> <p>For example, Ludtke discloses comparing biometric input of user with an existing record.</p> <p><i>See, e.g.,</i></p> <pre> graph TD Start([Start 3102]) --> Detect{Detect Fingerprint? 3104} Detect -- No --> Start Detect -- Yes --> Match{Does it match stored? 3106} Match -- No --> Error[Output Error Message 3110] Error --> Detect Match -- Yes --> Access[Access Function of Digital Wallet 3108] </pre> <p align="center">FIG. 31</p> <p><i>Id.</i> at Fig. 31.</p>

Exhibit 905-Y
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Ludtke

		<p>“FIG. 31 illustrates one embodiment of a method to securely and conveniently store and transmit telephony-based data. At 3102 the user may start a device, such as a digital wallet (DW). At 3104 the DW checks to see if a fingerprint has been detected. If not then the DW loops back looking for a fingerprint. If a fingerprint has been detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint. If a match does not occur, then at 3110 an error message is output and the DW returns to checking to see if a fingerprint has been detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes.” <i>Id.</i> at 39:47-59.</p>
1D	responsive to a determination that the scan data matches the biometric data,	<p>Ludtke discloses responsive to a determination that the scan data matches the biometric data.</p> <p>For example, Ludtke discloses taking action only if acquired biometric data matches the stored biometric template.</p> <p><i>See, e.g.,</i></p>

Exhibit 905-Y
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Ludtke

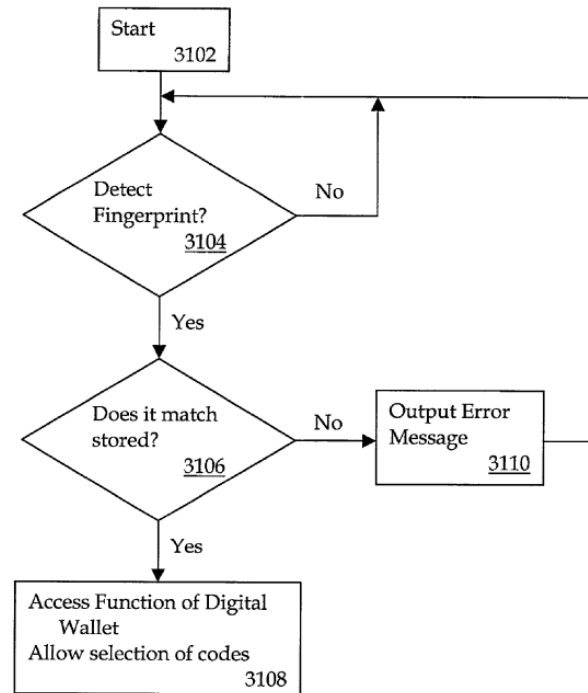


FIG. 31

Id. at Fig. 31.

“FIG. 31 illustrates one embodiment of a method to securely and conveniently store and transmit telephony-based data. At 3102 the user may start a device, such as a digital wallet (DW). At 3104 the DW checks to see if a fingerprint has been detected. If not then the DW loops back looking for a fingerprint. If a fingerprint has been detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint. If a match does not occur, then at 3110 an error message is output and the DW returns to checking to see if a fingerprint has been detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes.”

Exhibit 905-Y
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Ludtke

		<i>Id.</i> at 39:47-59.
1E	wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and	<p>Ludtke discloses wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority.</p> <p>For example, Ludtke discloses sending transaction device information to a transaction processing [or privacy] clearing house (TCPH) which maintains a secure database of transaction device information and user information.</p> <p><i>See, e.g.,</i></p> <div style="text-align: center;"> <p>COMMERCE GENERAL ARCHITECTURE</p> <p>FIG. 1</p> <p><i>Id.</i> at Fig. 1.</p> </div>

Exhibit 905-Y
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Ludtke

		<p>“One embodiment of a system is illustrated in FIG. 1. In this embodiment, a transaction privacy clearing house (TPCH) 110 interfaces a user 120 and a vendor 125. In this particular embodiment, a transaction device, e.g., a privacy card 130, is used to maintain the privacy of the user while enabling the user to perform transactions. The transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed.</p> <p>In order to maintain confidentiality of the identity of the user, the transaction device information does not provide user identification information. Thus, the vendor or other entities do not have user information but rather transaction device information. The TPCH 110 maintains a secure database of transaction device information and user information.”</p> <p><i>Id.</i> at 6:36-51.</p> <p>“In one embodiment of electronic distribution, the TPCH 110 functions as the middleman of the distribution channel. This allows the TPCH 110 to retain user privacy by not exposing addressing information and possibly email addresses to third parties.”</p> <p><i>Id.</i> at 7:44-48.</p> <p>“The TPCH 110 maintains a secure database of transaction device information and user information. In one embodiment, the TPCH 110 interfaces to at least one financial processing system 140 to perform associated financial transactions, such as confirming sufficient funds to perform the transaction, and transfers to the vendor 125 the fees required to complete the transaction.”</p> <p><i>Id.</i> at 6:49-55.</p> <p>“In one embodiment, the transaction device may be configured to closely resemble a standard credit card. More particularly, the card may have a magnetic stripe or a smart card chip that functions similarly to standard credit cards. In addition, the transaction device may contain wireless data communication, data storage and communication protocols for selectively communicating with outside devices such as a digital wallet described herein,</p>
--	--	---

Exhibit 905-Y
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Ludtke

		<p>point of sale (POS) terminal or personal computer (PC) and digital televisions (DTV).” <i>Id.</i> at 5:36-44.</p> <p>“A variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc.” <i>Id.</i> at 9:39-42.</p>
1F	<p>responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code,</p>	<p>Ludtke discloses responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code.</p> <p>For example, Ludtke discloses transmitting a signal (or a notification) from the TPCB to the transaction device when device information is confirmed.</p> <p><i>See, e.g.,</i></p> <p>“The transaction device information is provided to the TPCB 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed.” <i>Id.</i> at 6:41-44.</p>

Exhibit 905-Y
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Ludtke

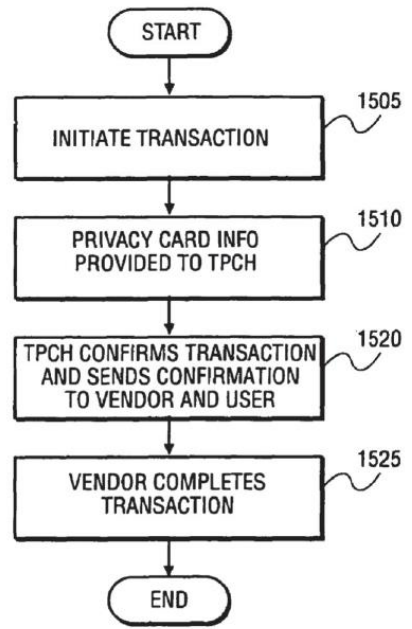
		 <p align="center">FIG. 15</p> <p><i>Id.</i> at Fig. 15.</p> <p>“The TPCH, at step 1520, confirms the transaction and provides the confirmation to the vendor and the user. At step 1525 the vendor completes the transaction without knowledge of the identity of the user.”</p> <p><i>Id.</i> at 27:13-16.</p>
1G	allowing the user to complete a financial transaction.	<p>Ludtke discloses allowing the user to complete a financial transaction.</p> <p>For example, Ludtke discloses approving financial transaction when device information is confirmed.</p>

Exhibit 905-Y
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Ludtke

		<p><i>See, e.g.,</i></p> <p>“The eCommerce system acts as a financial transaction middleman, stripping off user identity information from transactions. As a result, the user's private information is not stored in several databases across the Internet and in private business networks (e.g. grocery store networks).” <i>Id.</i> at 4:54-58.</p> <p>“The TPCH 110 maintains a secure database of transaction device information and user information. In one embodiment, the TPCH 110 interfaces to at least one financial processing system 140 to perform associated financial transactions, such as confirming sufficient funds to perform the transaction, and transfers to the vendor 125 the fees required to complete the transaction. In addition, the TPCH 110 may also provide information through a distribution system 150 that, in one embodiment, can provide a purchased product to the user 120, again without the vendor 125 knowing the identification of the user 120. In an alternate embodiment, the financial processing system need not be a separate entity but may be incorporated with other functionality. For example, in one embodiment, the financial processing system 140 may be combined with the TPCH 110 functionality.</p> <p>In one embodiment, the financial processing system (FP) 140 performs tasks of transferring funds between the user's account and the vendor's account for each transaction. In one embodiment, the presence of the TPCH 110 means that no details of the transactions, other than the amount of the transactions and other basic information, are known to the FP 140. The TPCH 110 issues transaction authorizations to the FP 140 function on an anonymous basis on behalf of the user over a highly secure channel. The FP 140 does not need to have many electronic channels receiving requests for fund transfer, as in a traditional financial processing system. In one embodiment, a highly secure channel is set up between the TPCH 110 and the FP 140; thus, the FP 140 is less vulnerable to spoofing.” <i>Id.</i> at 6:49-7:11.</p>
--	--	---

Exhibit 905-Y
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Ludtke

		<p>“One embodiment of a system is illustrated in FIG. 1. In this embodiment, a transaction privacy clearing house (TPCH) 110 interfaces a user 120 and a vendor 125. In this particular embodiment, a transaction device, e.g., a privacy card 130, is used to maintain the privacy of the user while enabling the user to perform transactions. The transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed.</p> <p>In order to maintain confidentiality of the identity of the user, the transaction device information does not provide user identification information. Thus, the vendor or other entities do not have user information but rather transaction device information. The TPCH 110 maintains a secure database of transaction device information and user information.”</p> <p><i>Id.</i> at 6:36-51.</p>
4	<p>The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris Scan, a hand geometry, a facial recognition, a signature recognition and a Voice recognition.</p>	<p>Ludtke discloses wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris Scan, a hand geometry, a facial recognition, a signature recognition and a Voice recognition.</p> <p>For example, Ludtke discloses a number of different types of biometric information that may be used to secure the device.</p> <p><i>See, e.g.,</i></p> <p>“Alternately, authentication may be achieved by using more sophisticated technologies such as a biometric solution (e.g., fingerprint recognition).”</p> <p><i>Id.</i> at 4:65-5:1.</p> <p>“In one embodiment, fingerprint recognition is used as a security mechanism that limits access to the card 705 to authorized users. A fingerprint touch pad and associated logic 730 is therefore included in one embodiment to perform these functions. Alternately, security may be achieved using a smart card chip</p>

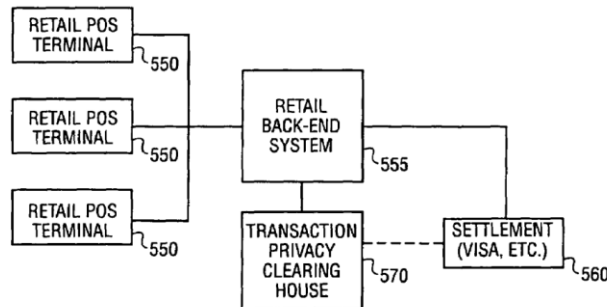
Exhibit 905-Y
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Ludtke

		<p>interface 750, which uses known smart card technology to perform the function.” <i>Id.</i> at 12:23-29.</p> <p>“FIG. 24 illustrates one embodiment of the system being utilized in a telephony based application. A standard telephone 2402 is interfaced via a telephone cable to, for example, a PBX, etc. The biometric device 2404 is integrated into the telephone 2402. In one example of operation, the user of the telephone 2402 is identified by the biometric device 2404 as an authorized user. Once identified as an authorized user, the biometric device 2404, may for example allow the user to use the telephone 2402. In another example, the biometric device 2404 may, once an authorized user is identified, allow transmission of tones representing such things as telephone numbers, access codes, PINs, etc.</p> <p>The identification by the biometric device may be achieved in a variety of ways, as discussed above. For example, biometric identification, may be, fingerprint, retinal scan, voice, DNA, hand profile, face recognition, etc.” <i>Id.</i> at 35:49-64.</p>
5	<p>The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.</p>	<p>Ludtke render obvious wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.</p> <p>For example, Ludtke discloses the transaction devices can be a digital wallet. Although, Johnson does not disclose the use of a mobile phone, tablet, or laptop it would be obvious to include it in this way.</p> <p><i>See, e.g.,</i></p> <p>“In addition, in one embodiment in which multiple transaction devices, e.g., a privacy card and a digital wallet, are used, it may be desirable to configure the first device to enable and program the second device in a secure manner.”</p>

Exhibit 905-Y
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Ludtke

		<i>Id.</i> at 5:1-5.
7	The method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.	<p>Ludtke discloses completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.</p> <p>For example, Ludtke discloses that access would be given applications of either computer software, a file (or both).</p> <p><i>See, e.g.,</i></p> <p style="text-align: center;">FIG. 5A</p> <p><i>Id.</i> at Fig. 5A.</p>

Exhibit 905-Y
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Ludtke



AN ALTERNATIVE EMBODIMENT OF THE RETAIL SYSTEM
 MODIFIED TO SUPPORT THE INTERACTION OF LEGACY POS
 TERMINALS WITH THE DIGITAL WALLET SYSTEM

FIG. 5B

Id. at Fig. 5B.

“As noted above, it is contemplated that the transaction device would operate in a home environment as well as in a retail environment. FIG. 5 a is a simplified block diagram of a retail system modified to support the interaction of a legacy POS terminal with a transaction device. The terminal 510 interfaces to TPCH 515 which communicates with the financial provider, for example, a credit card company 520, and the particular retailer 525. Alternately, as shown in FIG. 5 b, the POS terminal 550 interfaces to the retail system 555, which then interfaces with the credit card company 560 and the TPCH 570.

It is contemplated that the transaction device will be compatible with a variety of eCommerce system's POS terminals and therefore will provide magnetic stripe, barcode information and/or smart card chip. The magnetic stripe on the card or digital wallet can be programmed to represent a new account; thus a single transaction device may be configured to represent a number of different accounts.”

Id. at 9:7-25.

See also 1G.

9pre	An integrated device comprising:	Ludtke discloses an integrated device.
------	----------------------------------	--

Exhibit 905-Y
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Ludtke

		<i>See 1pre.</i>
9A	a persistent storage media that persistently stores biometric data of a user and an ID code;	Ludtke discloses a persistent storage media that persistently stores biometric data of a user and an ID code. <i>See IA.</i>
9B	a validation module, coupled to communicate with the persistent storage media,	Ludtke discloses a validation module, coupled to communicate with the persistent storage media, <i>See 1B-1C.</i>
9C	that receives scan data from a biometric scan for comparison against the biometric data,	Ludtke discloses receiving scan data from a biometric scan for comparison against the biometric data. <i>See 1B-1C.</i>
9D	and that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and	Ludtke discloses sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority. <i>See 1E.</i>
9E	a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and	Ludtke discloses a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third-party trusted authority Successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to-complete a financial transaction. <i>See 1E.</i>
9F	allowing the user to-complete a financial transaction.	Ludtke discloses allowing the user to-complete a financial transaction.

Exhibit 905-Y
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Ludtke

		<i>See 1F</i>
10	The integrated device of claim 7, wherein the ID code is transmitted to the third-party trusted authority over a network.	<p>Ludtke discloses the ID code is transmitted to the third-party trusted authority over a network</p> <p>For example, Ludtke discloses transmitting transaction device information over the Internet.</p> <p><i>See, e.g.,</i></p> <p>“The transaction device information is provided to the TPC 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed.” <i>Id.</i> at 6:41-44.</p> <p>“In one embodiment, the transaction device may be configured to closely resemble a standard credit card. More particularly, the card may have a magnetic stripe or a smart card chip that functions similarly to standard credit cards. In addition, the transaction device may contain wireless data communication, data storage and communication protocols for selectively communicating with outside devices such as a digital wallet described herein, point of sale (POS) terminal or personal computer (PC) and digital televisions (DTV).” <i>Id.</i> at 5:36-44.</p> <p>“A variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc.” <i>Id.</i> at 9:39-42.</p>
12	The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop,	<p>Ludtke discloses the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.</p> <p><i>See 5.</i></p>

Exhibit 905-Y
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Ludtke

	mp3 player, mobile gaming device, watch and a key fob.	
--	--	--

Exhibit 905-Z
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Okereke

US Patent Publication No. 2003/0196084 (“Okereke”) was filed on April 11, 2003 and published on October 16, 2003, and therefore qualifies as prior art under at least 35 U.S.C. §§ 102(a), (b), and (e) as to the asserted claims of U.S. Pat. No. 8,352,905 (“the ’905 Patent”). Okereke, including any material incorporated by reference into Okereke, anticipates claims 1, 4-5, 7, 9, 10, and 12 (“the Asserted Claims”) of the ’905 Patent under 35 U.S.C. § 102. Okereke also renders obvious the Asserted Claims under 35 U.S.C. § 103, alone based on the state of the art and/or in combination with one or more references identified in Samsung’s accompanying disclosure for the ’905 Patent.¹

To the extent Plaintiff alleges that Okereke does not disclose any particular limitation of the Asserted Claims of the ’905 Patent, either expressly or inherently, it would have been obvious to a person of ordinary skill in the art as of the priority date of the ’905 Patent to modify the Okereke reference and/or to combine the teachings of the Okereke reference with other prior art references, including but not limited to the present prior art references found in Exhibits 905-A-Y and the corresponding section(s) of charts for other prior art references for the ’905 Patent in a manner that would have rendered the Asserted Claims invalid as obvious.

With respect to the obviousness of the Asserted Claims under 35 U.S.C. § 103, one or more of the principles enumerated by the United States Supreme Court in *KSR v. Teleflex*, 550 U.S. 398 (2007) apply, including: (a) combining various claimed elements known in the prior art according to known methods to yield a predictable result; and/or (b) making a simple substitution of one or more known elements for another to obtain a predictable result; and/or (c) using a known technique to improve a similar device or method in the same way; and/or (d) applying a known technique to a known device or method ready for improvement to yield a predictable result; and/or (e) choosing from a finite number of identified, predictable solutions with a reasonable expectation of success or, in other words, the solution was one which was “obvious to try”; and/or (f) a known work in one field of endeavor prompting variations of it for use either in the same field or a different field based on given design incentives or other market forces in which the variations were predictable to one of ordinary skill in the art; and/or (g) a teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill in the art to modify the prior art reference or to combine the teachings of various prior art references to arrive at the claimed invention. It therefore would have been obvious to one of ordinary skill in the art to combine the disclosures of these references in accordance with the principles and rationales set forth above.

¹ Samsung notes that Plaintiff appears in many instances to be pursuing overly broad constructions of various limitations of the asserted claims of the ’905 Patent in an effort to piece together an infringement claim where none exists and to accuse a product that does not practice the claims. This claim chart may take into account Plaintiff’s overly broad constructions of the claim limitations. Any assertion that a particular limitation is disclosed by a prior art reference may be based on Plaintiff’s apparent constructions and is not intended to be, and is not, an admission that such constructions are supportable or proper.

Exhibit 905-Z**Invalidity Chart for U.S. Patent No. 9,298,905 In View of Okereke**

The citations to portions of any reference in this chart are exemplary only. For example, a citation that refers to or discusses a figure or figure item should be understood to also incorporate by reference that figure and any additional descriptions of that figure as if set forth fully therein. Samsung reserves the right to rely on the entirety of the references cited in this chart to show that the Asserted Claims are invalid. Citations presented for one claim limitation are expressly incorporated by reference into all other limitations for that claim as well as all limitations of all claims on which that claim depends. Samsung also reserves the right to rely on additional citations or sources of evidence that also may be applicable, or that may become applicable in light of claim construction, changes in Plaintiff's infringement contentions, and/or information obtained during discovery as the case progresses.

Claim	U.S. Patent No. 9,298,905	Exemplary Disclosure in Okereke
1 pre	A method comprising:	The Preamble is not limiting.
1 A	persistently storing biometric data of a legitimate user and an ID code on an integrated device;	<p>Okereke discloses persistently storing biometric data of a legitimate user and an ID code on an integrated device.</p> <p>For example, Okereke discloses using of fingerprint authentication and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device in the form of a serial number or SIM number and a private/public key process.</p> <p><i>See, e.g.,</i></p> <p>“The establishment of mobile access to secure resources in accordance with the present invention can occur as shown in FIGS. 4 and 5. The proxy server can be provided with software designed in accordance with the present invention, and a thin client application can be installed and/or downloaded onto the user's desktop computer. The proxy server program then awaits the initiation of a request 210 from the desktop to establish secure wireless access capabilities using the system of the present invention. In so doing, a unique identifier for the wireless product to be employed is passed as at 210 to the proxy server 125 program for authorization. The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other device capable of</p>

Exhibit 905-Z
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Okereke

		<p>remote wireless communication. The unique identifier can be a serial number or SIM. number, for example. If the unique identifier is one which the proxy server program identifies as being acceptable, the proxy server program will send approval as at 220 to the desktop 140, which executes functionality to make a key exchange as at 225, such as, for example, a Diffie Hellman Key Exchange. This key is used to encrypt information sent to the server using AES (Advanced Encryption Standard). AES is an encryption algorithm used by U.S. government agencies for securing sensitive but unclassified communications. In the preferred embodiment, this key is used to encrypt communication between the desktop and the server. In another embodiment, this key is used as part of a shared secret between the server and the client. This shared secret is used to generate a session key. The new session key ensures that conversations cannot be eavesdropped if the key has been compromised. The shared secret eliminates the possibility of a man-in-the-middle attack.”</p> <p><i>Id.</i> at ¶25.</p> <p>“The credential information or authentication measure can be something the user has (such as a swipe card), something the user is (such as represented by a fingerprint scan), or something the user knows (such as a password or pass phrase)”</p> <p><i>Id.</i> at ¶26.</p> <p>“The desktop computer includes a memory, processor, user interface, keyboard and mouse as is commonly known, and is preferably connected to a local area network (LAN) 175 for communication and use of shared resources as is commonly known. The user may be provided with a system PKI certificate 180 and private key for use with the desktop computer, in order to access and communicate to the extent authorized by the network administrator.”</p> <p><i>Id.</i> at ¶24.</p>
1B	responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a	Okereke discloses responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor.

Exhibit 905-Z
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Okereke

	<p>biometric scan performed by the biometric sensor;</p>	<p>For example, Okereke discloses using biometric verification – including a fingerprint – to verify the user of the device.</p> <p><i>See, e.g.,</i></p> <p>“The wireless device 165 is provided with a memory, processor, and input/output means as is commonly known. Using the session key, the user can then encrypt credential information, its PKI certificate 180 and private key, and forward this information to the proxy server 125 as at 230 in FIGS. 4 and 5. In one embodiment of the invention, the encrypted information is sent to the proxy server via secure IP network. The credential information or authentication measure can be something the user has (such as a swipe card), something the user is (such as represented by a fingerprint scan), or something the user knows (such as a password or pass phrase). In one embodiment, the credential information is a user name and password. In another embodiment of the invention, the credential information is a random number generated by programming on the wireless device, wherein the number changes in predetermined time intervals and is synchronized with programming on the proxy server so as to always match the corresponding number maintained on the proxy server.”</p> <p><i>Id.</i> at ¶26.</p> <p>“In one embodiment of the invention, desktop software is used to authenticate the user to the CPS, register the wireless device with the CPS, facilitate the initial key exchange and transfer the certificate and private key to the server. When the user wishes to access a resource from the wireless device outside of the secure network demarcation line (102 in FIG. 3), they are prompted for a second means of authentication, which may be something the user has (such as a swipe card, synchronized password keychain or channel key, for example), something the user is (such as a fingerprint scan), or something the user knows (such as a password or pass phrase). In a preferred embodiment this second</p>
--	--	---

Exhibit 905-Z
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Okereke

		form of authentication is something the user knows. The CPS verifies both forms of authentication, locates the user's certificate and establishes a session.” <i>Id.</i> at ¶32.
1C	comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;	<p>Okereke discloses comparing the scan data to the biometric data to determine whether the scan data matches the biometric data.</p> <p>For example, Okereke discloses using biometric verification – including a fingerprint – to verify the user of the device.</p> <p><i>See, e.g.,</i></p> <p>“The wireless device 165 is provided with a memory, processor, and input/output means as is commonly known. Using the session key, the user can then encrypt credential information, its PKI certificate 180 and private key, and forward this information to the proxy server 125 as at 230 in FIGS. 4 and 5. In one embodiment of the invention, the encrypted information is sent to the proxy server via secure IP network. The credential information or authentication measure can be something the user has (such as a swipe card), something the user is (such as represented by a fingerprint scan), or something the user knows (such as a password or pass phrase). In one embodiment, the credential information is a user name and password. In another embodiment of the invention, the credential information is a random number generated by programming on the wireless device, wherein the number changes in predetermined time intervals and is synchronized with programming on the proxy server so as to always match the corresponding number maintained on the proxy server.” <i>Id.</i> at ¶26.</p> <p>“In one embodiment of the invention, desktop software is used to authenticate the user to the CPS, register the wireless device with the CPS, facilitate the initial key exchange and transfer the certificate and private key to the server. When the user wishes to access a resource from the wireless device outside of</p>

Exhibit 905-Z
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Okereke

		<p>the secure network demarcation line (102 in FIG. 3), they are prompted for a second means of authentication, which may be something the user has (such as a swipe card, synchronized password keychain or channel key, for example), something the user is (such as a fingerprint scan), or something the user knows (such as a password or pass phrase). In a preferred embodiment this second form of authentication is something the user knows. The CPS verifies both forms of authentication, locates the user's certificate and establishes a session.” <i>Id.</i> at ¶32.</p>
1D	responsive to a determination that the scan data matches the biometric data,	<p>Okereke discloses responsive to a determination that the scan data matches the biometric data.</p> <p>For example, Okereke discloses taking action only if fingerprint is verified.</p> <p><i>See, e.g.,</i></p> <p>“As shown in FIG. 1, there is provided a traditional PKI system 10. The end user from the client workstation 20 sends a request 25 for a secure resource 50, and before access is granted, the user is requested 35 to provide a digital certificate 30 for authentication. The secure resource can be data, applications or other information of value. In some cases, once the digital certificate 30 is provided 40 and verified 55 by a certificate authority 60, access to the secure resource 50 will be granted as at 45. In other cases, an additional form of authentication may be required, such as a user name and password, a smart card, or a fingerprint, for example. The digital certificate verification process occurs through a certificate authority 60, normally a trusted third party.” <i>Id.</i> at ¶21.</p> <p>“In one embodiment of the invention, desktop software is used to authenticate the user to the CPS, register the wireless device with the CPS, facilitate the initial key exchange and transfer the certificate and private key to the server. When the user wishes to access a resource from the wireless device outside of the secure network demarcation line (102 in FIG. 3), they are prompted for a</p>

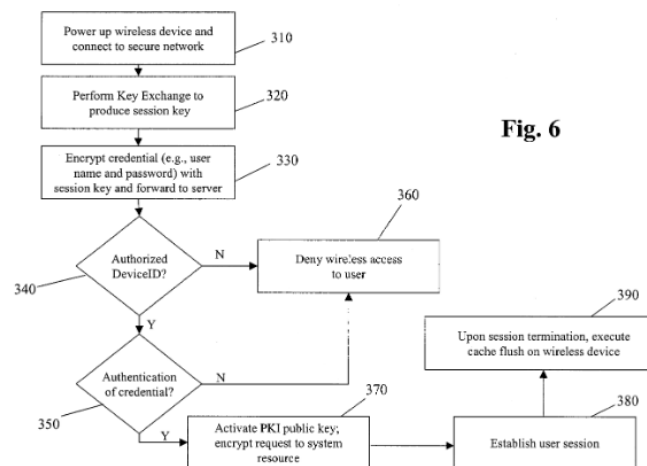
Exhibit 905-Z
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Okereke

		<p>second means of authentication, which may be something the user has (such as a swipe card, synchronized password keychain or channel key, for example), something the user is (such as a fingerprint scan), or something the user knows (such as a password or pass phrase). In a preferred embodiment this second form of authentication is something the user knows. The CPS verifies both forms of authentication, locates the user's certificate and establishes a session.” <i>Id.</i> at ¶32.</p>
1E	<p>wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and</p>	<p>Okereke discloses wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority.</p> <p>For example, Okereke discloses wirelessly sending a unique identifier of a wireless device to a proxy server program for authorization, where the proxy server possess a list of unique identifiers belonging to devices that are registered with the server.</p> <p><i>See, e.g.,</i></p> <p style="text-align: right;">Fig. 4</p> <p><i>Id.</i> at Fig. 4.</p> <p>“The establishment of mobile access to secure resources in accordance with the present invention can occur as shown in FIGS. 4 and 5. The proxy server can be provided with software designed in accordance with the present invention, and a thin client application can be installed and/or downloaded onto the user's desktop computer. The proxy server program then awaits the initiation of a</p>

Exhibit 905-Z
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Okereke

request 210 from the desktop to establish secure wireless access capabilities using the system of the present invention. In so doing, a unique identifier for the wireless product to be employed is passed as at 210 to the proxy server 125 program for authorization. The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other device capable of remote wireless communication. The unique identifier can be a serial number or SIM. number, for example. If the unique identifier is one which the proxy server program identifies as being acceptable, the proxy server program will send approval as at 220 to the desktop 140, which executes functionality to make a key exchange as at 225, such as, for example, a Diffie Hellman Key Exchange.”

Id. at ¶25.



Id. at Fig. 6.

“If the user is authenticated by the proxy server matching the device unique identifier with authorized device identifications as at 340, and the credential information is authenticated as determined at 350, the proxy server will activate the user's PKI public key and request the secure network resource for the user, as at 370.”

Exhibit 905-Z
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Okereke

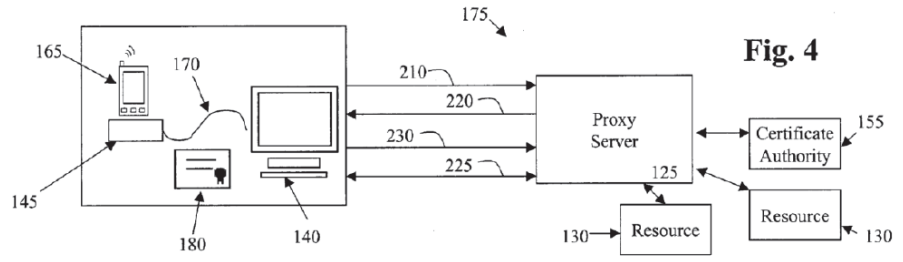
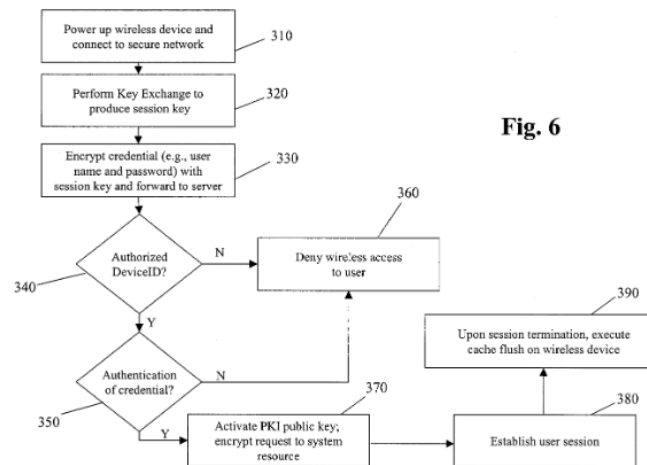
		<p><i>Id.</i> at ¶28.</p> <p>“The user can ensure secure communication between the wireless device and the Certificate Proxy Server (CPS) in various ways, including physically connecting the device to the server, or connecting securely over a known trusted network. As the user's certificate and private key are securely transferred to the CPS, the unique network identifier for the user's wireless device (such as a SIM number) is registered with the server. This network identifier registration can also be done in a number of ways, including over the wireless network, or over a physical network.”</p> <p><i>Id.</i> at ¶30.</p>
1F	responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code,	<p>Okereke discloses responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code.</p> <p>For example, Okereke discloses sending approval message from proxy server to devices and allow user session to begin after the devices and users are verified taking action only if the users or the devices are authenticated by the proxy server.</p> <p><i>See, e.g.,</i></p>  <p style="text-align: right;">Fig. 4</p> <p><i>Id.</i> at Fig. 4.</p>

Exhibit 905-Z
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Okereke

“The establishment of mobile access to secure resources in accordance with the present invention can occur as shown in FIGS. 4 and 5. The proxy server can be provided with software designed in accordance with the present invention, and a thin client application can be installed and/or downloaded onto the user's desktop computer. The proxy server program then awaits the initiation of a request 210 from the desktop to establish secure wireless access capabilities using the system of the present invention. In so doing, a unique identifier for the wireless product to be employed is passed as at 210 to the proxy server 125 program for authorization. The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other device capable of remote wireless communication. The unique identifier can be a serial number or SIM. number, for example. If the unique identifier is one which the proxy server program identifies as being acceptable, the proxy server program will send approval as at 220 to the desktop 140, which executes functionality to make a key exchange as at 225, such as, for example, a Diffie Hellman Key Exchange.”

Id. at ¶25.



Id. at Fig. 6.

Exhibit 905-Z
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Okereke

		<p>“If the user is authenticated by the proxy server matching the device unique identifier with authorized device identifications as at 340, and the credential information is authenticated as determined at 350, the proxy server will activate the user's PKI public key and request the secure network resource for the user, as at 370.” <i>Id.</i> at ¶28.</p> <p>“The user can ensure secure communication between the wireless device and the Certificate Proxy Server (CPS) in various ways, including physically connecting the device to the server, or connecting securely over a known trusted network. As the user's certificate and private key are securely transferred to the CPS, the unique network identifier for the user's wireless device (such as a SIM number) is registered with the server. This network identifier registration can also be done in a number of ways, including over the wireless network, or over a physical network.” <i>Id.</i> at ¶30.</p>
1G	allowing the user to complete a financial transaction.	<p>Okereke discloses allowing the user to complete a financial transaction.</p> <p>For example, Okereke discloses its system can be implemented in a financial transaction process.</p> <p><i>See, e.g.,</i></p> <p>“Both private and public entities rely on information technology systems to perform essential or mission-critical functions. Some computer information, such as defense, financial, medical, and personnel data, is sensitive and merits special or additional protection against unauthorized use or disclosure. As information technology becomes increasingly distributed and interconnected, the consequences of losing control of information become greater. For example, systems that perform electronic financial transactions or electronic commerce must protect against unauthorized access to confidential records and unauthorized modification of data. Sometimes, the value of the information lies</p>

Exhibit 905-Z
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Okereke

		<p>in its limited distribution; wide spread knowledge and misuse could reduce the value of that information. In other cases, release of the information could lead to extrinsic harm, such as a violation of personal privacy. Easy access to sensitive information may also lead to malicious corruption of the information. Yet the distributed, collaborative, and open nature of early networks, including the Internet, encouraged the free flow of information in a manner that is not suited to information control.”</p> <p><i>Id.</i> at ¶3.</p>
5	<p>The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.</p>	<p>Okereke discloses wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.</p> <p>For example, Okereke discloses personal digital assistant (PDA), laptop, and cellular telephone.</p> <p><i>See, e.g.,</i></p> <p>“The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other device capable of remote wireless communication. The unique identifier can be a serial number or SIM. number, for example.”</p> <p><i>Id.</i> at ¶25.</p>
4	<p>The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris Scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.</p>	<p>Okereke discloses wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris Scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.</p> <p>For example, Okereke discloses using fingerprint to secure the device.</p> <p><i>See, e.g.,</i></p> <p>“In other cases, an additional form of authentication may be required, such as a user name and password, a smart card, or a fingerprint, for example.”</p>

Exhibit 905-Z
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Okereke

		<p><i>Id.</i> at ¶21.</p> <p>“The credential information or authentication measure can be something the user has (such as a swipe card), something the user is (such as represented by a fingerprint scan), or something the user knows (such as a password or pass phrase)”</p> <p><i>Id.</i> at ¶26.</p>
7	<p>The method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.</p>	<p>Okereke discloses wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.</p> <p>For example, Okereke discloses that access would be given applications of either computer software, a file (or both).</p> <p><i>See, e.g.,</i></p> <div style="text-align: center;"> <p>Fig. 6</p> </div> <p><i>Id.</i> at Fig. 6.</p>

Exhibit 905-Z
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Okereke

		<p>“If the user is authenticated by the proxy server matching the device unique identifier with authorized device identifications as at 340, and the credential information is authenticated as determined at 350, the proxy server will activate the user's PKI public key and request the secure network resource for the user, as at 370. If the device identification is not authorized, or the user's credential is not authenticated, access to the user will be denied as at 360. The proxy server will then receive the request for digital certificate and private key, and provide the previously stored digital certificate and key, which can then be validated by the certificate authority, and the user's session can begin.”</p> <p><i>Id.</i> at ¶28.</p> <p><i>See also</i> 1G.</p>
9pre	An integrated device comprising:	<p>Okereke discloses an integrated device.</p> <p><i>See</i> 1pre.</p>
9A	a persistent storage media that persistently stores biometric data of a user and an ID code;	<p>Okereke discloses a persistent storage media that persistently stores biometric data of a user and an ID code.</p> <p><i>See</i> 1A.</p>
9B	a validation module, coupled to communicate with the persistent storage media,	<p>Okereke discloses a validation module, coupled to communicate with the persistent storage media,</p> <p><i>See</i> 1B-1C.</p>
9C	that receives scan data from a biometric scan for comparison against the biometric data,	<p>Okereke discloses receiving scan data from a biometric scan for comparison against the biometric data.</p> <p><i>See</i> 1B-1C.</p>

Exhibit 905-Z
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Okereke

9D	and that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and	Okereke discloses sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority. <i>See 1E.</i>
9E	a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and	Okereke discloses a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third-party trusted authority Successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to-complete a financial transaction. <i>See 1E.</i>
9F	allowing the user to-complete a financial transaction.	Okereke discloses allowing the user to-complete a financial transaction. <i>See 1F</i>
10	The integrated device of claim 7, wherein the ID code is transmitted to the third-party trusted authority over a network.	Okereke discloses wherein the ID code is transmitted to the third-party trusted authority over a network. For example, Okereke discloses transmitting device identifier over the Internet. <i>See, e.g.,</i> “In a specific embodiment as shown in FIG. 4, the user is first provided with a network-connected device, such as a desktop computer 140, along with one or more docking stations 145. One or more wireless-capable devices 165 may be docked in the docking station for two-way communication with the desktop computer as indicated at 170. The desktop computer includes a memory, processor, user interface, keyboard and mouse as is commonly known, and is

Exhibit 905-Z
Invalidity Chart for U.S. Patent No. 9,298,905 In View of Okereke

		<p>preferably connected to a local area network (LAN) 175 for communication and use of shared resources as is commonly known.” <i>Id.</i> at ¶24.</p> <p>“The proxy server can be provided with software designed in accordance with the present invention, and a thin client application can be installed and/or downloaded onto the user's desktop computer. The proxy server program then awaits the initiation of a request 210 from the desktop to establish secure wireless access capabilities using the system of the present invention. In so doing, a unique identifier for the wireless product to be employed is passed as at 210 to the proxy server 125 program for authorization. The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other device capable of remote wireless communication. The unique identifier can be a serial number or SIM. number, for example.” <i>Id.</i> at ¶25.</p>
12	The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.	<p>Okereke discloses the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.</p> <p><i>See 5.</i></p>

Exhibit 989-X
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Johnson

US Patent No. 7,849,020 (“Johnson”) was filed March 15, 2006 and claims priority to April 19, 2005 and to the extend the ’989 Patent is found to not be entitled to priority date earlier than its application date, therefore qualifies as prior art under at least 35 U.S.C. §§ 102(a), (b), and (e) as to the asserted claims of U.S. Pat. No. 10,698,989 (“the ’989 Patent”). Johnson, including any material incorporated by reference into Johnson, anticipates claims 1-6 (“the Asserted Claims”) of the ’989 Patent under 35 U.S.C. § 102. Johnson also renders obvious the Asserted Claims under 35 U.S.C. § 103, alone based on the state of the art and/or in combination with one or more references identified in Samsung’s accompanying disclosure for the ’989 Patent.¹

To the extent Plaintiff alleges that Johnson does not disclose any particular limitation of the Asserted Claims of the ’989 Patent, either expressly or inherently, it would have been obvious to a person of ordinary skill in the art as of the priority date of the ’989 Patent to modify the Johnson reference and/or to combine the teachings of the Johnson reference with other prior art references, including but not limited to the present prior art references found in Exhibits 989-A-W and 989-Y-Z and the corresponding section(s) of charts for other prior art references for the ’989 Patent in a manner that would have rendered the Asserted Claims invalid as obvious.

With respect to the obviousness of the Asserted Claims under 35 U.S.C. § 103, one or more of the principles enumerated by the United States Supreme Court in *KSR v. Teleflex*, 550 U.S. 398 (2007) apply, including: (a) combining various claimed elements known in the prior art according to known methods to yield a predictable result; and/or (b) making a simple substitution of one or more known elements for another to obtain a predictable result; and/or (c) using a known technique to improve a similar device or method in the same way; and/or (d) applying a known technique to a known device or method ready for improvement to yield a predictable result; and/or (e) choosing from a finite number of identified, predictable solutions with a reasonable expectation of success or, in other words, the solution was one which was “obvious to try”; and/or (f) a known work in one field of endeavor prompting variations of it for use either in the same field or a different field based on given design incentives or other market forces in which the variations were predictable to one of ordinary skill in the art; and/or (g) a teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill in the art to modify the prior art reference or to combine the teachings of various prior art references to arrive at the claimed invention. It therefore would have been obvious to one of ordinary skill in the art to combine the disclosures of these references in accordance with the principles and rationales set forth above.

¹ Samsung notes that Plaintiff appears in many instances to be pursuing overly broad constructions of various limitations of the asserted claims of the ’989 Patent in an effort to piece together an infringement claim where none exists and to accuse a product that does not practice the claims. This claim chart may take into account Plaintiff’s overly broad constructions of the claim limitations. Any assertion that a particular limitation is disclosed by a prior art reference may be based on Plaintiff’s apparent constructions and is not intended to be, and is not, an admission that such constructions are supportable or proper.

Exhibit 989-X
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Johnson

The citations to portions of any reference in this chart are exemplary only. For example, a citation that refers to or discusses a figure or figure item should be understood to also incorporate by reference that figure and any additional descriptions of that figure as if set forth fully therein. Samsung reserves the right to rely on the entirety of the references cited in this chart to show that the Asserted Claims are invalid. Citations presented for one claim limitation are expressly incorporated by reference into all other limitations for that claim as well as all limitations of all claims on which that claim depends. Samsung also reserves the right to rely on additional citations or sources of evidence that also may be applicable, or that may become applicable in light of claim construction, changes in Plaintiff's infringement contentions, and/or information obtained during discovery as the case progresses.

Claim	U.S. Patent No. 10,698,989	Exemplary Disclosure in Johnson
1 pre	A method comprising:	The Preamble is not limiting.
1A	receiving, at a smartphone, an identification (ID) code from a third-party trusted authority, the ID code uniquely identifying the smartphone among a plurality of smartphones;	<p>Johnson renders obvious receiving, at a smartphone, an identification (ID) code from a third-party trusted authority, the ID code uniquely identifying the smartphone among a plurality of smartphones.</p> <p>For example, Johnson discloses persistent storage of user specific information and tokens carrying device specific information such as a SIM number. While Johnson does not disclose the use of smartphone, it would be obvious to include.</p> <p><i>See, e.g.,</i></p> <p>“In one embodiment, various elements of an online transaction are distributed over separate and independent network entities. For example, the identity provider may provide identity validation in the form of an identity token, which the merchant can use to verify the identity of the purchaser. The identity token may include one or more identity credentials of the end-user. The identity token may be issued based on the identity information provided by the end-user/purchaser, for example, the subscribe number from the SIM card, a</p>

Exhibit 989-X
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Johnson

		<p>network address (e.g., a Network Interface Card (NIC) identification, World Wide Name (WWN), etc.), login information, etc. Similarly, the payment provider may provide verification of the end-user's ability to pay in the form of a payment token. In addition, the payment provider may handle payment transactions on behalf of the purchaser in satisfaction of the purchase of goods and/or services from the merchant. The above described framework allows, inter alia, a purchaser and merchant that are strangers to conduct an online commercial transaction in an untrusted network environment in relative confidence, as discussed in further detail in the various exemplary embodiments provided below.” <i>Id.</i> at 6:7-27.</p> <p>“To obtain an identity token, end-user 140 provides identity information to identity provider 120. Identity information may include any information that enables the identity provider 120 to distinguish between end-user utilizing end-user computer 110 and the various other end-users to which identity provider may provide services. For example, the identity information may include a unique identifier associated with the hardware of end-user computer 110. In one embodiment, the identity information is provided by a SIM card issuing an identifier unique to the subscriber. Identity information may include providing a unique hardware number of the network interface card (NIC) of the end-user computer 110, a world wide name (WWN) or other network address of end-user computer 110 or any other means by which end-user computer 110 may be identified, including (in some embodiments) an established login name/password combination.” <i>Id.</i> at 7:57-8:4.</p>
1B	persistently storing biometric data and the ID code on the smartphone, wherein the biometric data is one selected from a group consisting of facial recognition, a	Johnson renders obvious persistently storing biometric data and the ID code on the smartphone, wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan of a legitimate user.

Exhibit 989-X
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Johnson

	<p>fingerprint scan, and a retinal scan of a legitimate user;</p>	<p>Although, Johnson does not disclose the use of biometrics it would be obvious to include it in this way.</p> <p><i>See, e.g.,</i></p> <p>“The identity provider 120 may transmit the identity token to end-user computer 110 to forward to merchant 140 (step 235), and/or identity provider 120 may transmit the identity token directly to the merchant 140. Merchant 140 may then process the identity token to identify end-user and/or to verify that end-user is who he/she purports to be. The identity token may be used to authenticate certain information about the end-user that may affect the transaction. For example, the merchant 140 may provide a service that requires the end-user to be of a certain age. Identity credentials transmitted with the identity token may be used to ensure that the end-user is of the proper age and meets this requirement. Merchant 140 may have discounts for particular end-users that are frequent purchasers, or who received a coupon, promotional offer, etc. The merchant 140 may index a database of end-users to determine whether the end-user qualifies or should otherwise be specially handled based on the provided identity credentials.</p> <p>Optionally, the merchant 140 may request validation of the identity token by sending a request to the identity provider 120 (step 245). The request for validation of the identity token may include forwarding the identity token from merchant 140 to identity provider 120. Upon receiving the request for validation of the identity token, the identity provider 120 may validate the identity token, and thereby determine whether the identity token is authentic. The identity provider 120 may then forward an indication of the validity of the identity token to the merchant 140 (step 255). Alternatively, the merchant 140 may simply validate the identity token itself (step 265) (e.g., by assuming the identity token is valid or otherwise processing the token).</p> <p>Optionally, a response may be returned from the merchant 140 to the end-user computer 110, where the response may include a message of whether the</p>
--	---	--

Exhibit 989-X
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Johnson

identity token is valid, of any applicable discount or promotional offers, and/or any other type of message, as the invention is not limited in this respect (step **265**).” *Id.* at 8:46-9:14.

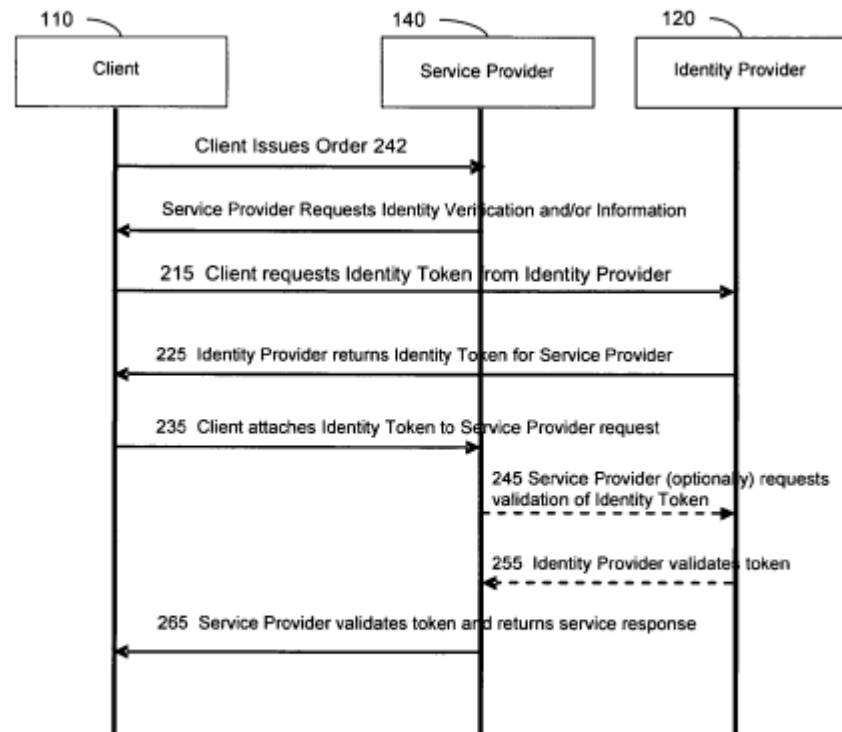


FIG. 2

Exhibit 989-X
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Johnson

1C	receiving, at the smartphone, scan data from a biometric scan using the smartphone;	<p>Johnson renders obvious receiving, at the smartphone, scan data from a biometric scan using the smartphone.</p> <p>Although, Johnson does not disclose the use of biometrics it would be obvious to include it in this way.</p> <p><i>See, e.g.,</i></p> <p>“The identity provider 120 may transmit the identity token to end-user computer 110 to forward to merchant 140 (step 235), and/or identity provider 120 may transmit the identity token directly to the merchant 140. Merchant 140 may then process the identity token to identify end-user and/or to verify that end-user is who he/she purports to be. The identity token may be used to authenticate certain information about the end-user that may affect the transaction. For example, the merchant 140 may provide a service that requires the end-user to be of a certain age. Identity credentials transmitted with the identity token may be used to ensure that the end-user is of the proper age and meets this requirement. Merchant 140 may have discounts for particular end-users that are frequent purchasers, or who received a coupon, promotional offer, etc. The merchant 140 may index a database of end-users to determine whether the end-user qualifies or should otherwise be specially handled based on the provided identity credentials.</p> <p>Optionally, the merchant 140 may request validation of the identity token by sending a request to the identity provider 120 (step 245). The request for validation of the identity token may include forwarding the identity token from merchant 140 to identity provider 120. Upon receiving the request for validation of the identity token, the identity provider 120 may validate the identity token, and thereby determine whether the identity token is authentic. The identity provider 120 may then forward an indication of the validity of the identity token to the merchant 140 (step 255). Alternatively, the merchant 140 may simply validate the identity token itself (step 265) (e.g., by</p>
----	---	--

Exhibit 989-X
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Johnson

assuming the identity token is valid or otherwise processing the token). Optionally, a response may be returned from the merchant **140** to the end-user computer **110**, where the response may include a message of whether the identity token is valid, of any applicable discount or promotional offers, and/or any other type of message, as the invention is not limited in this respect (step **265**).” *Id.* at 8:46-9:14.

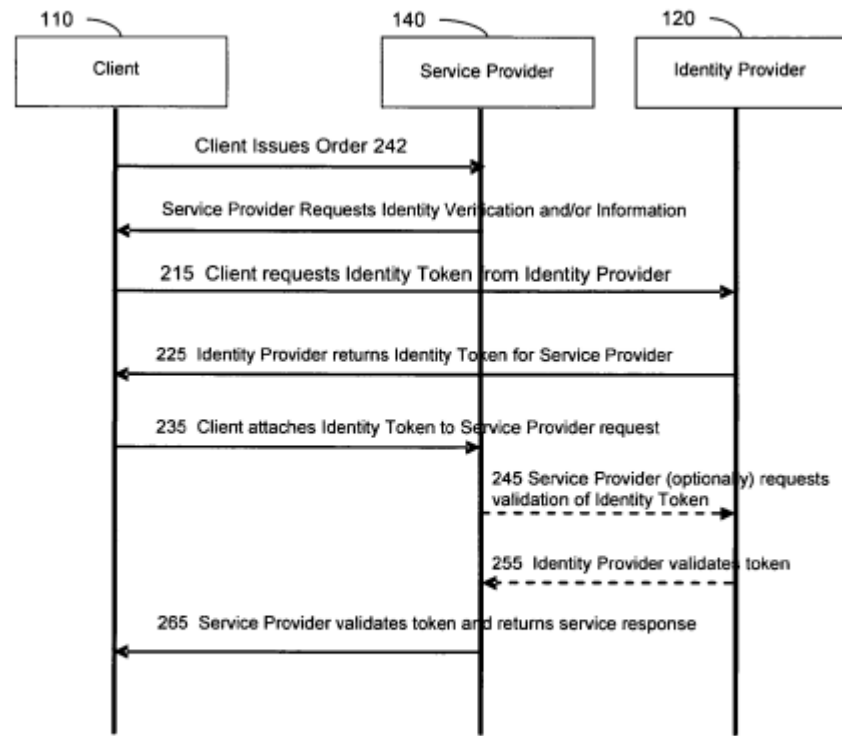


FIG. 2

Exhibit 989-X
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Johnson

1D	comparing, using the smartphone, the scan data to the biometric data;	<p>Johnson renders obvious comparing, using the smartphone, the scan data to the biometric data.</p> <p>Although, Johnson does not disclose the use of biometrics it would be obvious to include it in this way.</p> <p><i>See, e.g.,</i></p> <p>“The identity provider 120 may transmit the identity token to end-user computer 110 to forward to merchant 140 (step 235), and/or identity provider 120 may transmit the identity token directly to the merchant 140. Merchant 140 may then process the identity token to identify end-user and/or to verify that end-user is who he/she purports to be. The identity token may be used to authenticate certain information about the end-user that may affect the transaction. For example, the merchant 140 may provide a service that requires the end-user to be of a certain age. Identity credentials transmitted with the identity token may be used to ensure that the end-user is of the proper age and meets this requirement. Merchant 140 may have discounts for particular end-users that are frequent purchasers, or who received a coupon, promotional offer, etc. The merchant 140 may index a database of end-users to determine whether the end-user qualifies or should otherwise be specially handled based on the provided identity credentials.</p> <p>Optionally, the merchant 140 may request validation of the identity token by sending a request to the identity provider 120 (step 245). The request for validation of the identity token may include forwarding the identity token from merchant 140 to identity provider 120. Upon receiving the request for validation of the identity token, the identity provider 120 may validate the identity token, and thereby determine whether the identity token is authentic. The identity provider 120 may then forward an indication of the validity of the</p>

Exhibit 989-X
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Johnson

		<p>identity token to the merchant 140 (step 255). Alternatively, the merchant 140 may simply validate the identity token itself (step 265) (e.g., by assuming the identity token is valid or otherwise processing the token). Optionally, a response may be returned from the merchant 140 to the end-user computer 110, where the response may include a message of whether the identity token is valid, of any applicable discount or promotional offers, and/or any other type of message, as the invention is not limited in this respect (step 265).” <i>Id.</i> at 8:46-9:14.</p>
--	--	--

Exhibit 989-X
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Johnson

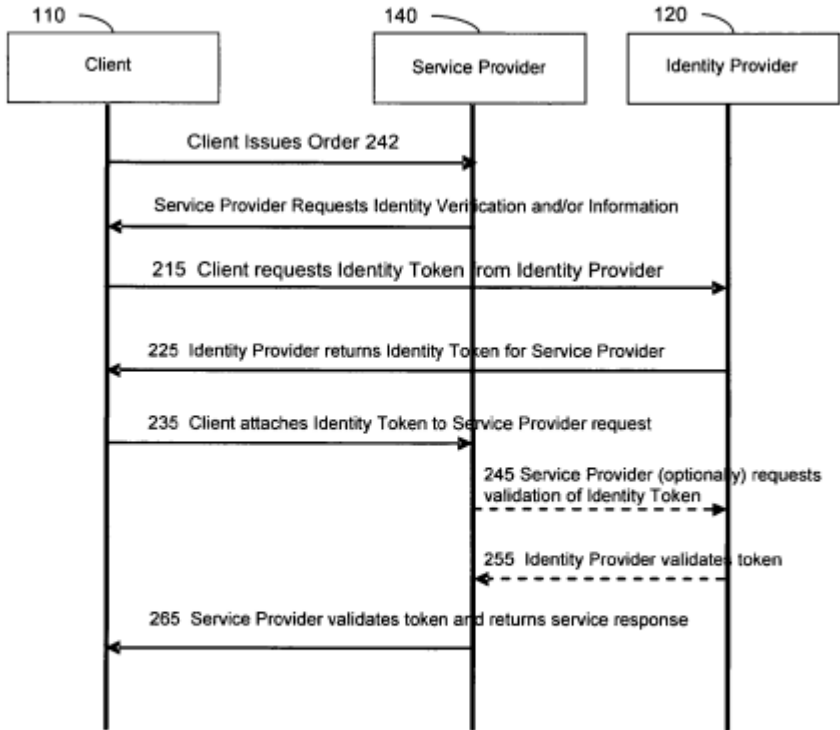
		 <pre> sequenceDiagram participant 110 as Client participant 140 as Service Provider participant 120 as Identity Provider 110->>140: Client Issues Order 242 140->>110: Service Provider Requests Identity Verification and/or Information 110->>120: 215 Client requests Identity Token from Identity Provider 120->>140: 225 Identity Provider returns Identity Token for Service Provider 110->>140: 235 Client attaches Identity Token to Service Provider request 140->>120: 245 Service Provider (optional) requests validation of Identity Token 120->>140: 255 Identity Provider validates token 140->>110: 265 Service Provider validates token and returns service response </pre> <p align="center">FIG. 2</p>
1E	determining whether the scan data matches the biometric data; and	<p>Johnson renders obvious responsive to a determination that the scan data matches the biometric data.</p> <p><i>See 1D.</i></p>

Exhibit 989-X
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Johnson

1F	responsive to a determination that the scan data matches the biometric data	<p>Johnson renders obvious responsive to a determination that the scan data matches the biometric data.</p> <p><i>See</i> 1D.</p>
1G	wirelessly sending, from the smartphone, the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority	<p>Johnson discloses wirelessly sending, from the smartphone, the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority.</p> <p>For example, Johnson discloses sending device IDs and other information and codes to a central database for verification.</p> <p><i>See, e.g.,</i></p> <p>“An end-user computer 110 may place an order 242 with a merchant 140. The order 242 may be any indication that the end-user would like to purchase one or more goods and/or services from the merchant 140. For example, the order 242 may result from end-user selecting a good or service via a web browser displaying pages resident at the website of a merchant, or may result from choosing an option from an application running locally, as described in further detail below. As an example of the first instance, the merchant 140 may provide a website to display or otherwise offer for sale goods and/or services that it provides, or may provide an online catalog of merchandise. The order 242 may be any type of indication that end-user would like to purchase one or more goods and/or services from the merchant 140.</p> <p>As an example of the second instance and as an alternative to selecting one or more goods and services from a merchant's website, order 242 may originate from an application or other program local to the end-user computer 110. For example, an end user may create, produce or edit a document via a word processing application, design a slide show using a presentation application</p>

Exhibit 989-X
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Johnson

		<p>and/or manipulate images or graphics for a poster or brochure using an imaging application. The application may include an option under the print menu that allows the document to be printed by a third party to, for example, take advantage of printing features that may not be locally available, or to otherwise exploit professional printing services. When the option is selected, the application may send, via the network, order 242 to the merchant 140. It should be appreciated that order 242 may be any indication to purchase any good and/or service, as the aspects of the invention are not limited in this respect.</p> <p>In response to order 242, merchant 140 may request that end-user 110 provide an indication of the end-user's identity and/or verification that the end-user is indeed who he/she purports to be (step 205). For example, merchant 140 may not know anything about the source of order 242 and may desire information about the identity of the end-user and/or assurance that the end-user is not spoofing his/her identity. Alternatively, the merchant 140 may send a notice or indication that payment is required for the service and demand that a payment token be provided. To obtain a payment token, it may be necessary to first establish an identity via an identity token, as described in further detail below. In either case, end-user 110 may respond to the request by the merchant 140 by enlisting the services of identity provider 120 (step 215).” <i>Id.</i> 7:11-7:55.</p> <p>“From the perspective of the merchant, the commercial transaction is substantially risk free as the identity of the end-user and the payment verification is handled by third parties and is therefore less susceptible to fraud, spoofing and even innocent mistakes in providing personal and financial information. Therefore, merchants may be more willing to conduct online commercial transactions with unknown end-users over an untrusted network. From the perspective of the end-user, personal and financial information resides with entities either that already maintain the information and/or that the end-user has an established relationship with. Confidential personal and financial end-user information need not be provided to the merchant, mitigating the</p>
--	--	---

Exhibit 989-X
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Johnson

		<p>vulnerabilities of having confidential information misused or misappropriated. As a result, end-users may be more willing to conduct commercial transactions with unknown merchants without having to worry about whether the merchant is trustworthy or not.</p> <p>In some conventional commercial transaction models, identity information and payment information are input by the user and processed by either a third party or the merchant. As discussed above, these models are awkward, inefficient and time consuming for the user. In addition, conventional models present numerous issues regarding security of an end-user's confidential information as well as making a merchant vulnerable to fraud and/or susceptible to failure to pay by an end-user. Applicant has appreciated that commercial transaction software installed on each of the computers employed in various commercial transactions may mitigate or eliminate concerns over security and fraud. In addition, many of the actions handled by the end-user and merchant in conventional models may be performed by the commercial transactions software, making the transaction simpler and more intuitive to the end-user.” <i>Id.</i> at 10:47-11:12.</p>
1H	a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code	<p>Johnson discloses a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code.</p> <p>For example, Johnson discloses transmitting an authentication output and allow transaction following verification of user and devices.</p> <p><i>See, e.g.,</i></p> <p>“The identity provider 120 may transmit the identity token to end-user computer 110 to forward to merchant 140 (step 235), and/or identity provider 120 may transmit the identity token directly to the merchant 140.</p>

Exhibit 989-X
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Johnson

	<p>Merchant 140 may then process the identity token to identify end-user and/or to verify that end-user is who he/she purports to be. The identity token may be used to authenticate certain information about the end-user that may affect the transaction. For example, the merchant 140 may provide a service that requires the end-user to be of a certain age. Identity credentials transmitted with the identity token may be used to ensure that the end-user is of the proper age and meets this requirement. Merchant 140 may have discounts for particular end-users that are frequent purchasers, or who received a coupon, promotional offer, etc. The merchant 140 may index a database of end-users to determine whether the end-user qualifies or should otherwise be specially handled based on the provided identity credentials.</p> <p>Optionally, the merchant 140 may request validation of the identity token by sending a request to the identity provider 120 (step 245). The request for validation of the identity token may include forwarding the identity token from merchant 140 to identity provider 120. Upon receiving the request for validation of the identity token, the identity provider 120 may validate the identity token, and thereby determine whether the identity token is authentic. The identity provider 120 may then forward an indication of the validity of the identity token to the merchant 140 (step 255). Alternatively, the merchant 140 may simply validate the identity token itself (step 265) (e.g., by assuming the identity token is valid or otherwise processing the token).</p> <p>Optionally, a response may be returned from the merchant 140 to the end-user computer 110, where the response may include a message of whether the identity token is valid, of any applicable discount or promotional offers, and/or any other type of message, as the invention is not limited in this respect (step 265).</p> <p>After the merchant 140 has processed the identity token and/or has received a validation for the identity token from the identity provider 120, the merchant 140 may request that the end-user provide verification or validation of an ability to pay and/or provide an indication of how the end-user would like to pay for the goods or services. The merchant 140 may make the request via a</p>
--	---

Exhibit 989-X
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Johnson

		<p>payment token request (step 305 in FIG. 3). In response to the payment token request, the end-user computer 110 may enlist the services of a payment provider 130. Payment provider 130 may be associated with a third party that maintains financial and payment information about various end-users, such as a financial institution, or a third party broker that handles financial transactions and payment procedures.</p> <p>The end-user computer 110 may solicit a payment token from a payment provider 130 (step 315) by transmitting the identity token to payment provider 130. Alternatively, the end-user may request a payment token by logging onto the payment provider 130 in a manner similar to that discussed in connection with the identity provider 120 (i.e., by providing an identifier such as a SIM subscriber number, NIC address and/or using a login/password combination). It should be appreciated that the end-user may request a payment token in other ways, as the invention is not limited in this respect. In addition, the end-user may send information about the purchase, such as the price and nature of the purchase so that the payment provider can verify that the end-user is capable of paying. However, providing purchase information is not required, as it may not be necessary or it may be handled in subsequent steps of the transaction.” <i>Id.</i> at 8:46-9:44</p> <p>“In one embodiment, the local installation of the commercial transaction software 485 a on identity provider 420 can create an identity token identifying the end-user utilizing end-user computer 410. Furthermore, the commercial transaction software 485 a on identity provider 420 can forward the identity token to the end-user computer 410, the payment provider 430, the merchant 440, and/or any other computer, as the invention is not limited in this respect. The local installation of the commercial transaction software 485 b on the end-user computer 410 can issue identity information (so as to identify the end-user) in response to an indication to conduct an online transaction between the end-user and a merchant. The local installation of the commercial transaction software 485 c installed on payment provider 430 can receive the</p>
--	--	--

Exhibit 989-X
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Johnson

	<p>identity token and generate a payment token verifying an ability of the end-user to pay (e.g., the payment token) for the online transaction. The local installation of the commercial transaction software 485 <i>d</i> installed on the merchant 440 can receive the verification of the ability of the end-user to pay before proceeding with the online transaction.</p> <p>In one embodiment, each of the computers in system 400 operates using a local installation of a same or similar operating system 495. For example, each of the computers in system 400 may operate using the Microsoft Windows® operating system. Commercial transactions software 485 may be a subsystem of the operating system. In this way, the various computers employed in a commercial transaction communicate in a consistent and known fashion. Since the commercial transactions software is communicating directly over the network and handling the validation, verification and security, the end-user and merchant need not know anything about one another, and more importantly, may not need to establish any trust relationship. In addition, because certain portions of the transactions are handled by the operating system, much of the transaction may be performed substantially invisible to the user, without requiring confusing and often times awkward involvement by the end-user. By having the commercial transactions software on each computer, various encryption techniques may be used during transmission of information from one computer to another. Moreover, further security features may be included such as identity tokens and/or payment tokens that are valid for a limited time period. For example, an identity token may include a time component that specifies a time after which any component receiving and processing the token should deem it invalid, and not honor the token as verification of identity and/or payment. The commercial transactions software components may programmatically process any time limits associated with a token. This may prevent tokens obtained by “fishing” from being used inappropriately at a later date.” <i>Id.</i> at 11:34-12:16</p>
--	---

Exhibit 989-X
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Johnson

1I	<p>wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.</p>	<p>Johnson discloses wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.</p> <p><i>See</i> 1H.</p> <p>For example, Johnson discloses use of the system with an ATM, computer, and vending machine.</p> <p><i>See, e.g.,</i></p> <p>“The end-user computer 110 may solicit a payment token from a payment provider 130 (step 315) by transmitting the identity token to payment provider 130. Alternatively, the end-user may request a payment token by logging onto the payment provider 130 in a manner similar to that discussed in connection with the identity provider 120 (i.e., by providing an identifier such as a SIM subscriber number, NIC address and/or using a login/password combination). It should be appreciated that the end-user may request a payment token in other ways, as the invention is not limited in this respect. In addition, the end-user may send information about the purchase, such as the price and nature of the purchase so that the payment provider can verify that the end-user is capable of paying. However, providing purchase information is not required, as it may not be necessary or it may be handled in subsequent steps of the transaction.” <i>Id.</i> at 9:29-44</p> <p>“In one embodiment, each of the computers in system 400 operates using a local installation of a same or similar operating system 495. For example, each of the computers in system 400 may operate using the Microsoft Windows® operating system. Commercial transactions software 485 may be a subsystem of the operating system. In this way, the various computers employed in a commercial transaction communicate in a consistent and known fashion. Since</p>
----	--	--

Exhibit 989-X
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Johnson

		<p>the commercial transactions software is communicating directly over the network and handling the validation, verification and security, the end-user and merchant need not know anything about one another, and more importantly, may not need to establish any trust relationship. In addition, because certain portions of the transactions are handled by the operating system, much of the transaction may be performed substantially invisible to the user, without requiring confusing and often times awkward involvement by the end-user. By having the commercial transactions software on each computer, various encryption techniques may be used during transmission of information from one computer to another. Moreover, further security features may be included such as identity tokens and/or payment tokens that are valid for a limited time period. For example, an identity token may include a time component that specifies a time after which any component receiving and processing the token should deem it invalid, and not honor the token as verification of identity and/or payment. The commercial transactions software components may programmatically process any time limits associated with a token. This may prevent tokens obtained by “fishing” from being used inappropriately at a later date.” <i>Id.</i> at 11:54-12:16</p>
2A	The method of claim 1, further comprising: Receiving a request for biometric verification, and	<p>Johnson renders obvious receiving a request for biometric verification.</p> <p><i>See</i> 1C.</p>
2B	responsive to a determination that the scan data does not match the biometric data,	<p>Johnson renders obvious responsive to a determination that the scan data does not match the biometric data.</p> <p><i>See</i> 1C-D.</p>
2C	indicating the smartphone cannot verify the scan data as being from the legitimate user, the smartphone does not send the ID code.	<p>Johnson discloses indicating the device cannot verify the scan data as being from the legitimate user, the smartphone does not send the ID code.</p>

Exhibit 989-X
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Johnson

		<i>See 2B</i>
3	The method of claim 1, wherein completing the transaction includes accessing an application.	Johnson discloses transaction includes accessing an application. <i>See 1H.</i>
4A	The method of claim 1, wherein the transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code	Johnson discloses wherein the transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code. <i>See 1G-1H.</i>
4B	includes the third-party trusted authority sending an indication that the third-party trusted authority authenticated the ID code to another party.	Johnson discloses includes the third-party trusted authority sending an indication that the third-party trusted authority authenticated the ID code to another party. <i>See 1H.</i>
5pre	A smartphone comprising:	Johnson discloses a device. <i>See 1A.</i>
5A	a persistent storage having an input that receives an identification (ID) code from a third-party trusted authority, and biometric data	Johnson discloses a persistent storage having an input that receives an identification (ID) code from a third-party trusted authority, and biometric data. <i>See 1A.</i>
5B	wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan, of a legitimate user	Johnson discloses wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan, of a legitimate user. <i>See 1B.</i>

Exhibit 989-X
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Johnson

5C	the ID code uniquely identifying the smartphone among a plurality of smartphones	Johnson discloses the ID code uniquely identifying the device among a plurality of devices. <i>See 1A.</i>
5D	the persistent storage storing the biometric data and the ID code,	Johnson discloses the persistent storage storing the biometric data and the ID code. <i>See 1A.</i>
5E	the persistent storage having an output configured to provide a first set of biometric data and the ID code for use on the smartphone;	Johnson discloses the persistent storage having an output configured to provide a first set of biometric data and the ID code for use on the device. <i>See 1A.</i>
5F	a validation module, coupled to communicate with the persistent storage to receive the biometric data from the persistent storage,	Johnson renders obvious a validation module, coupled to communicate with the persistent storage to receive the biometric data from the persistent storage. <i>See 1D.</i>
5G	the validation module having a scan pad to capture scan data from a biometric scan,	Johnson renders obvious the validation module having a scan pad to capture scan data from a biometric scan. <i>See 1C-D.</i>
5H	the validation module comparing the scan data to the biometric data to determine whether the scan data matches the biometric data; and	Johnson renders obvious the validation module comparing the scan data to the biometric data to determine whether the scan data matches the biometric data. <i>See 1D.</i>
5I	a wireless transceiver that,	Johnson discloses a wireless transceiver. <i>See 1G.</i>

Exhibit 989-X
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Johnson

5J	responsive to a determination that the scan data matches the biometric data,	Johnson renders obvious responsive to a determination that the scan data matches the biometric data. <i>See</i> 1C-D.
5K	sends the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority,	Johnson discloses sends the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority. <i>See</i> 1G.
5L	a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code,	Johnson discloses a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code. <i>See</i> 1H.
5M	wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.	Johnson discloses wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account. <i>See</i> 1I.
6	The smartphone of claim 5, wherein the ID code is transmitted to the third-party trusted authority over a network.	Johnson discloses wherein the ID code is transmitted to the third-party trusted authority over a network For example, Johnson discloses communication for verification over the Internet. “Network 105 may be any type of network in any type of configuration that interconnects and allows nodes connected to the network to communicate. Nodes or devices may be connected to the network via copper (e.g., Category 5) cable, optical connections, wireless or any combination thereof. Information may be transferred using any low level protocol such as Ethernet and/or any

Exhibit 989-X
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Johnson

		information protocol such as TCP/IP. The network 105 may have any number of devices connected to it and may be a trusted (e.g., intranet) or an untrusted network (e.g., LAN/WAN, Internet, etc.), or a combination of both. The computers connected to the network may be any type of device including, but not limited to, one or any combination of a mobile phone, a desktop computer, a tablet personal computer, a server, workstation, etc.” <i>Id.</i> at 6:47-60.
--	--	---

Exhibit 989-Y
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Ludtke

US Patent No. 7,188,110 (“Ludtke”) was filed on December 11, 2000 and issued on March 6, 2007, and therefore qualifies as prior art under at least 35 U.S.C. §§ 102(a), (b), and (e) as to the asserted claims of U.S. Pat. No. 10,698,989 (“the ’989 Patent”). Ludtke, including any material incorporated by reference into Ludtke, anticipates claims 1-6 (“the Asserted Claims”) of the ’989 Patent under 35 U.S.C. § 102. Ludtke also renders obvious the Asserted Claims under 35 U.S.C. § 103, alone based on the state of the art and/or in combination with one or more references identified in Samsung’s accompanying disclosure for the ’989 Patent.¹

To the extent Plaintiff alleges that Ludtke does not disclose any particular limitation of the Asserted Claims of the ’989 Patent, either expressly or inherently, it would have been obvious to a person of ordinary skill in the art as of the priority date of the ’989 Patent to modify the Ludtke reference and/or to combine the teachings of the Ludtke reference with other prior art references, including but not limited to the present prior art references found in Exhibits 989-A-X and 989-Z and the corresponding section(s) of charts for other prior art references for the ’989 Patent in a manner that would have rendered the Asserted Claims invalid as obvious.

With respect to the obviousness of the Asserted Claims under 35 U.S.C. § 103, one or more of the principles enumerated by the United States Supreme Court in *KSR v. Teleflex*, 550 U.S. 398 (2007) apply, including: (a) combining various claimed elements known in the prior art according to known methods to yield a predictable result; and/or (b) making a simple substitution of one or more known elements for another to obtain a predictable result; and/or (c) using a known technique to improve a similar device or method in the same way; and/or (d) applying a known technique to a known device or method ready for improvement to yield a predictable result; and/or (e) choosing from a finite number of identified, predictable solutions with a reasonable expectation of success or, in other words, the solution was one which was “obvious to try”; and/or (f) a known work in one field of endeavor prompting variations of it for use either in the same field or a different field based on given design incentives or other market forces in which the variations were predictable to one of ordinary skill in the art; and/or (g) a teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill in the art to modify the prior art reference or to combine the teachings of various prior art references to arrive at the claimed invention. It therefore would have been obvious to one of ordinary skill in the art to combine the disclosures of these references in accordance with the principles and rationales set forth above.

The citations to portions of any reference in this chart are exemplary only. For example, a citation that refers to or discusses a figure or figure item should be understood to also incorporate by reference that figure and any additional descriptions of that figure as if set

¹ Samsung notes that Plaintiff appears in many instances to be pursuing overly broad constructions of various limitations of the asserted claims of the ’989 Patent in an effort to piece together an infringement claim where none exists and to accuse a product that does not practice the claims. This claim chart may take into account Plaintiff’s overly broad constructions of the claim limitations. Any assertion that a particular limitation is disclosed by a prior art reference may be based on Plaintiff’s apparent constructions and is not intended to be, and is not, an admission that such constructions are supportable or proper.

Exhibit 989-Y
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Ludtke

forth fully therein. Samsung reserves the right to rely on the entirety of the references cited in this chart to show that the Asserted Claims are invalid. Citations presented for one claim limitation are expressly incorporated by reference into all other limitations for that claim as well as all limitations of all claims on which that claim depends. Samsung also reserves the right to rely on additional citations or sources of evidence that also may be applicable, or that may become applicable in light of claim construction, changes in Plaintiff's infringement contentions, and/or information obtained during discovery as the case progresses.

Claim	U.S. Patent No. 10,698,989	Exemplary Disclosure in Ludtke
1pre	A method comprising:	The Preamble is not limiting.
1A	receiving, at a smartphone, an identification (ID) code from a third-party trusted authority, the ID code uniquely identifying the smartphone among a plurality of smartphones;	<p>Ludtke renders obvious receiving, at a smartphone, an identification (ID) code from a third-party trusted authority, the ID code uniquely identifying the smartphone among a plurality of smartphones.</p> <p>For example, Ludtke discloses providing device information to a transaction privacy clearing house (TPCH) for verification. Although Ludtke does not disclose receiving the device information from TPCH or the use of smartphone, it would be obvious to include it in this way.</p> <p><i>See, e.g.,</i> “One embodiment of a system is illustrated in FIG. 1. In this embodiment, a transaction privacy clearing house (TPCH) 110 interfaces a user 120 and a vendor 125. In this particular embodiment, a transaction device, e.g., a privacy card 130, is used to maintain the privacy of the user while enabling the user to perform transactions. The transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed.” <i>Id.</i> at 6:36-44.</p>

Exhibit 989-Y
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Ludtke

		<p>“The POS terminal can also be used to transfer data from the TPCCH to the transaction device. An example of data that may be transferred, is the distribution of electronic contents such as electronic coupons, which might pass directly from the TPCCH to the transaction device.” <i>Id.</i> at 21:57-62.</p> <p>“Such technology could be added to existing devices commonly used by shippers such as UPS or FedEx, which already employ bar code scanning devices to streamline and optimize their shipping operations. The distributor has already received the necessary data from the TPCCH which associates the user's physical address with the package ID, so the distributor's infrastructure processes the package as necessary, routing through delivery hubs, etc. The distributor takes the package to the user's physical address, step 1805.” <i>Id.</i> at 32:16-24.</p>
1B	persistently storing biometric data and the ID code on the smartphone, wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan of a legitimate user;	<p>Ludtke discloses persistently storing biometric data and the ID code on the smartphone, wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan of a legitimate user.</p> <p>For example, Ludtke discloses using transaction device information and storing fingerprint data in a tamper-proof format on the integrated transaction device.</p> <p><i>See, e.g.,</i></p> <p>“The fingerprint data entry process may be performed at least twice, to confirm that the user has entered the correct data (using the correct fingerprint). If confirmation succeeds, the device writes the fingerprint image data into write-once memory, or other memory that is protected from accidental modification.” <i>Id.</i> at 19:35-40.</p>

Exhibit 989-Y
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Ludtke

		<p>“The privacy card records the keys in its own permanent, secure memory. Thereafter, subsequent access to the privacy card by the user requires secure exchange between the card and digital wallet.” <i>Id.</i> at 21:46-50</p> <p>“One embodiment of a system is illustrated in FIG. 1. In this embodiment, a transaction privacy clearing house (TPCH) 110 interfaces a user 120 and a vendor 125. In this particular embodiment, a transaction device, e.g., a privacy card 130, is used to maintain the privacy of the user while enabling the user to perform transactions. The transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed.” <i>Id.</i> at 6:36-44.</p> <p>“Alternately, authentication may be achieved by using more sophisticated technologies such as a biometric solution (e.g., fingerprint recognition).” <i>Id.</i> at 4:65-5:1.</p> <p>“In one embodiment, fingerprint recognition is used as a security mechanism that limits access to the card 705 to authorized users. A fingerprint touch pad and associated logic 730 is therefore included in one embodiment to perform these functions. Alternately, security may be achieved using a smart card chip interface 750, which uses known smart card technology to perform the function.” <i>Id.</i> at 12:23-29.</p>
1C	receiving, at the smartphone, scan data from a biometric scan using the smartphone;	Ludtke renders obvious receiving, at the smartphone, scan data from a biometric scan using the smartphone.

Exhibit 989-Y
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Ludtke

For example, Ludtke discloses using biometric verification – including a fingerprint – to verify the user of the device. Although Ludtke does not disclose the use of smartphone, it would be obvious to include it in this way.

See, e.g.,

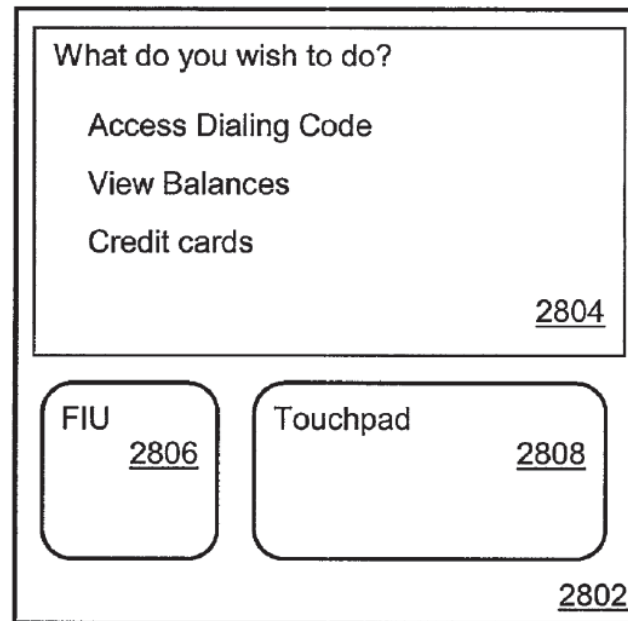


FIG. 28

Id. at Fig. 28.

“FIG. 28 illustrates one embodiment of a device, as a consumer access device, 2802 that implements the method discussed above. The consumer access device 2802 has an LCD screen 2804 showing text, a biometric identification unit, in this embodiment as a Fingerprint Identification Unit (FIU) 2806 and a touchpad

Exhibit 989-Y
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Ludtke

2808 for user input. The user of the consumer access device 2802 would be authorized access to the device 2802 if the device recognized the user after the user had pressed his finger against the FIU 2806.”
Id. at 39:19-27.

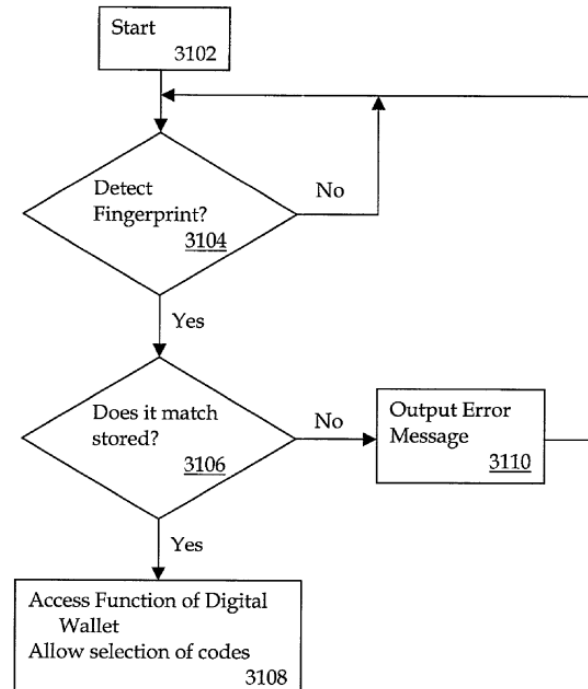


FIG. 31

Id. at Fig. 31.

“FIG. 31 illustrates one embodiment of a method to securely and conveniently store and transmit telephony-based data. At 3102 the user may start a device, such as a digital wallet (DW). At 3104 the DW checks to see if a fingerprint has

Exhibit 989-Y
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Ludtke

		<p>been detected. If not then the DW loops back looking for a fingerprint. If a fingerprint has been detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint. If a match does not occur, then at 3110 an error message is output and the DW returns to checking to see if a fingerprint has been detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes.” <i>Id.</i> at 39:47-59.</p>
1D	comparing, using the smartphone, the scan data to the biometric data;	<p>Ludtke discloses comparing, using the smartphone, the scan data to the biometric data.</p> <p>For example, Ludtke discloses comparing biometric input of user with an existing record.</p> <p><i>See, e.g.,</i></p>

Exhibit 989-Y
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Ludtke

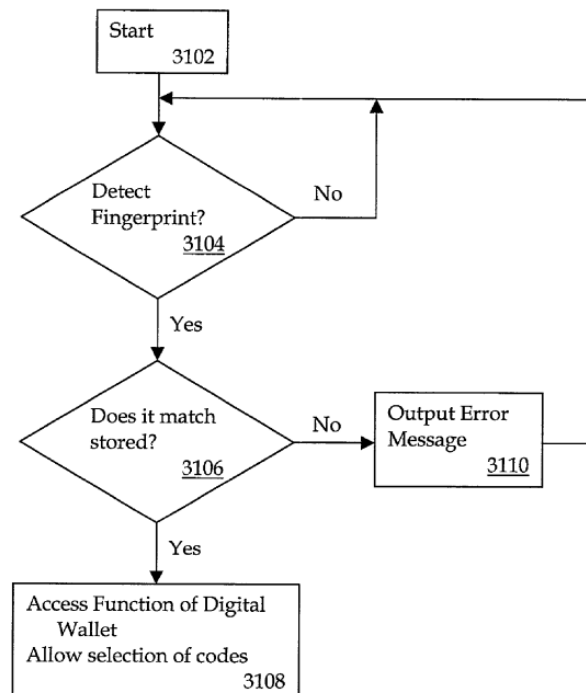


FIG. 31

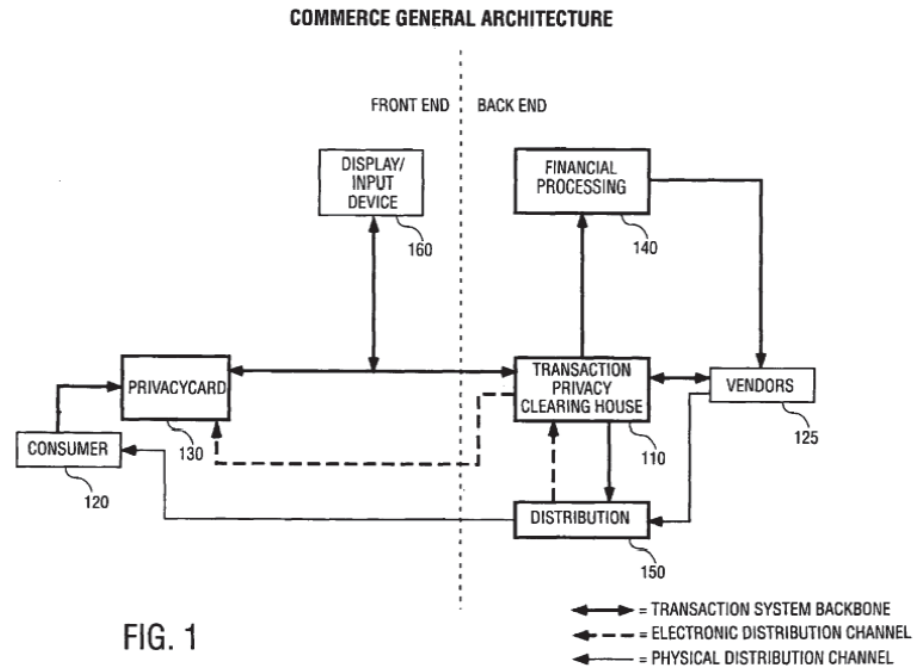
Id. at Fig. 31.

“FIG. 31 illustrates one embodiment of a method to securely and conveniently store and transmit telephony-based data. At 3102 the user may start a device, such as a digital wallet (DW). At 3104 the DW checks to see if a fingerprint has been detected. If not then the DW loops back looking for a fingerprint. If a fingerprint has been detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint. If a match does not occur, then at 3110 an error message is output and the DW returns to checking to see if a fingerprint has

Exhibit 989-Y
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Ludtke

		been detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes.” <i>Id.</i> at 39:47-59.
1E	determining whether the scan data matches the biometric data; and	Ludtke discloses responsive to a determination that the scan data matches the biometric data. <i>See</i> 1D.
1F	responsive to a determination that the scan data matches the biometric data	Ludtke discloses responsive to a determination that the scan data matches the biometric data. <i>See</i> 1D.
1G	wirelessly sending, from the smartphone, the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority	Ludtke renders obvious wirelessly sending, from the smartphone, the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority. For example, Ludtke discloses sending transaction device information to a transaction processing [or privacy] clearing house (TCPH) which maintains a secure database of transaction device information and user information. Although Ludtke does not disclose the use of smartphone, it would be obvious to include it in this way. <i>See, e.g.,</i>

Exhibit 989-Y
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Ludtke



Id. at Fig. 1.

“One embodiment of a system is illustrated in FIG. 1. In this embodiment, a transaction privacy clearing house (TPCH) 110 interfaces a user 120 and a vendor 125. In this particular embodiment, a transaction device, e.g., a privacy card 130, is used to maintain the privacy of the user while enabling the user to perform transactions. The transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed.”

Id. at 6:36-44.

“In one embodiment of electronic distribution, the TPCH 110 functions as the middleman of the distribution channel. This allows the TPCH 110 to retain user

Exhibit 989-Y
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Ludtke

		<p>privacy by not exposing addressing information and possibly email addresses to third parties.” <i>Id.</i> at 7:44-48.</p> <p>“The TPCCH 110 maintains a secure database of transaction device information and user information. In one embodiment, the TPCCH 110 interfaces to at least one financial processing system 140 to perform associated financial transactions, such as confirming sufficient funds to perform the transaction, and transfers to the vendor 125 the fees required to complete the transaction.” <i>Id.</i> at 6:49-55.</p> <p>“In one embodiment, the transaction device may be configured to closely resemble a standard credit card. More particularly, the card may have a magnetic stripe or a smart card chip that functions similarly to standard credit cards. In addition, the transaction device may contain wireless data communication, data storage and communication protocols for selectively communicating with outside devices such as a digital wallet described herein, point of sale (POS) terminal or personal computer (PC) and digital televisions (DTV).” <i>Id.</i> at 5:36-44.</p> <p>“A variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc.” <i>Id.</i> at 9:39-42.</p>
1H	a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code	<p>Ludtke discloses a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code.</p> <p>For example, Ludtke discloses transmitting a signal (or a notification) from the TPCCH to the transaction device when device information is confirmed so approval of the transaction to be performed.</p>

Exhibit 989-Y
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Ludtke

		<p><i>See, e.g.,</i></p> <p>“The transaction device information is provided to the TPCCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed.” <i>Id.</i> at 6:41-44.</p> <p>“The transaction device information is provided to the TPCCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed.” <i>Id.</i> at 6:41-44.</p>
--	--	--

Exhibit 989-Y
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Ludtke

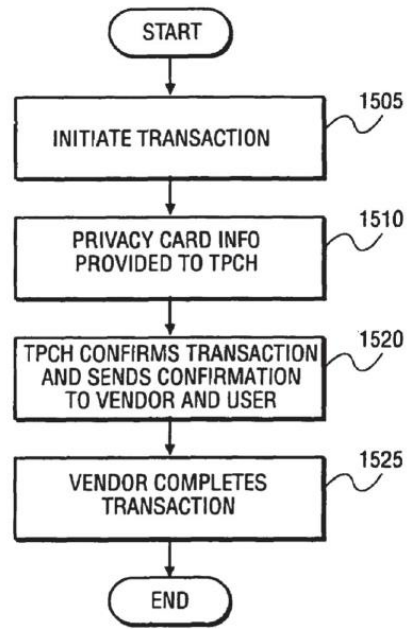
		 <p align="center">FIG. 15</p> <p><i>Id.</i> at Fig. 15.</p> <p>“The TPCH, at step 1520, confirms the transaction and provides the confirmation to the vendor and the user. At step 1525 the vendor completes the transaction without knowledge of the identity of the user.”</p> <p><i>Id.</i> at 27:13-16.</p>
1I	wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a	Ludtke discloses wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.

Exhibit 989-Y
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Ludtke

keyless lock, an ATM machine, a web site, a file and a financial account.

For example, Ludtke discloses that access would be given applications of either computer software, a file (or both).

See, e.g.,

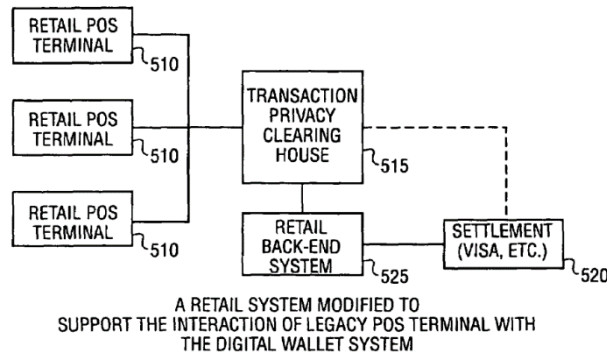


FIG. 5A

Id. at Fig. 5A.

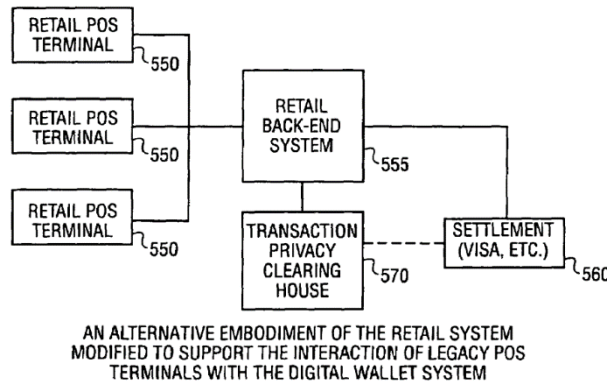


FIG. 5B

Id. at Fig. 5B.

Exhibit 989-Y
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Ludtke

		<p>“As noted above, it is contemplated that the transaction device would operate in a home environment as well as in a retail environment. FIG. 5 a is a simplified block diagram of a retail system modified to support the interaction of a legacy POS terminal with a transaction device. The terminal 510 interfaces to TPC 515 which communicates with the financial provider, for example, a credit card company 520, and the particular retailer 525. Alternately, as shown in FIG. 5 b, the POS terminal 550 interfaces to the retail system 555, which then interfaces with the credit card company 560 and the TPC 570.</p> <p>It is contemplated that the transaction device will be compatible with a variety of eCommerce system's POS terminals and therefore will provide magnetic stripe, barcode information and/or smart card chip. The magnetic stripe on the card or digital wallet can be programmed to represent a new account; thus a single transaction device may be configured to represent a number of different accounts.”</p> <p><i>Id.</i> at 9:7-25.</p>
2A	The method of claim 1, further comprising: Receiving a request for biometric verification, and	<p>Ludtke discloses receiving a request for biometric verification.</p> <p><i>See</i> 1C.</p>
2B	responsive to a determination that the scan data does not match the biometric data,	<p>Ludtke discloses responsive to a determination that the scan data does not match the biometric data.</p> <p><i>See, e.g.,</i></p> <p>“If a fingerprint has been detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint. If a match does not occur, then at 3110 an error message is output and the DW returns to checking to see if a fingerprint has been detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes.” <i>Id.</i> at 39:52-59.</p>

Exhibit 989-Y
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Ludtke

2C	indicating the smartphone cannot verify the scan data as being from the legitimate user, the smartphone does not send the ID code.	Ludtke discloses indicating the device cannot verify the scan data as being from the legitimate user, the smartphone does not send the ID code. <i>See 2B</i>
3	The method of claim 1, wherein completing the transaction includes accessing an application.	Ludtke discloses transaction includes accessing an application. <i>See 1H.</i>
4A	The method of claim 1, wherein the transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code	Ludtke discloses wherein the transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code. <i>See 1G-1H.</i>
4B	includes the third-party trusted authority sending an indication that the third-party trusted authority authenticated the ID code to another party.	Ludtke discloses includes the third-party trusted authority sending an indication that the third-party trusted authority authenticated the ID code to another party. <i>See 1H.</i>
5pre	A smartphone comprising:	Ludtke discloses a device. <i>See 1A.</i>
5A	a persistent storage having an input that receives an identification (ID) code from a third-party trusted authority, and biometric data	Ludtke discloses a persistent storage having an input that receives an identification (ID) code from a third-party trusted authority, and biometric data. <i>See 1A.</i>
5B	wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan, of a legitimate user	Ludtke discloses wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan, of a legitimate user. <i>See 1B.</i>

Exhibit 989-Y
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Ludtke

5C	the ID code uniquely identifying the smartphone among a plurality of smartphones	Ludtke discloses the ID code uniquely identifying the device among a plurality of devices. <i>See 1A.</i>
5D	the persistent storage storing the biometric data and the ID code,	Ludtke discloses the persistent storage storing the biometric data and the ID code. <i>See 1A.</i>
5E	the persistent storage having an output configured to provide a first set of biometric data and the ID code for use on the smartphone;	Ludtke discloses the persistent storage having an output configured to provide a first set of biometric data and the ID code for use on the device. <i>See 1A.</i>
5F	a validation module, coupled to communicate with the persistent storage to receive the biometric data from the persistent storage,	Ludtke discloses a validation module, coupled to communicate with the persistent storage to receive the biometric data from the persistent storage. <i>See 1C-D.</i>
5G	the validation module having a scan pad to capture scan data from a biometric scan,	Ludtke discloses the validation module having a scan pad to capture scan data from a biometric scan. <i>See 1C-D.</i>
5H	the validation module comparing the scan data to the biometric data to determine whether the scan data matches the biometric data; and	Ludtke discloses the validation module comparing the scan data to the biometric data to determine whether the scan data matches the biometric data. <i>See 1C-D.</i>
5I	a wireless transceiver that,	Ludtke discloses a wireless transceiver. <i>See 1G.</i>

Exhibit 989-Y
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Ludtke

5J	responsive to a determination that the scan data matches the biometric data,	Ludtke discloses responsive to a determination that the scan data matches the biometric data. <i>See</i> 1C-D.
5K	sends the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority,	Ludtke discloses sends the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority. <i>See</i> 1G.
5L	a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code,	Ludtke discloses a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code. <i>See</i> 1H.
5M	wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.	Ludtke discloses wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account. <i>See</i> 1I.
6	The smartphone of claim 5, wherein the ID code is transmitted to the third-party trusted authority over a network.	Ludtke discloses wherein the ID code is transmitted to the third-party trusted authority over a network. For example, Ludtke discloses transmitting transaction device information over the Internet. <i>See, e.g.,</i> “The transaction device information is provided to the TPC 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed.”

Exhibit 989-Y
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Ludtke

		<p><i>Id.</i> at 6:41-44.</p> <p>“In one embodiment, the transaction device may be configured to closely resemble a standard credit card. More particularly, the card may have a magnetic stripe or a smart card chip that functions similarly to standard credit cards. In addition, the transaction device may contain wireless data communication, data storage and communication protocols for selectively communicating with outside devices such as a digital wallet described herein, point of sale (POS) terminal or personal computer (PC) and digital televisions (DTV).”</p> <p><i>Id.</i> at 5:36-44.</p> <p>“A variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc.”</p> <p><i>Id.</i> at 9:39-42.</p>
--	--	---

Exhibit 989-Z
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Okereke

US Patent Publication No. 2003/0196084 (“Okereke”) was filed on April 11, 2003 and published on October 16, 2003, and therefore qualifies as prior art under at least 35 U.S.C. §§ 102(a), (b), and (e) as to the asserted claims of U.S. Pat. No. 10,698,989 (“the ’989 Patent”). Okereke, including any material incorporated by reference into Okereke, anticipates claims 1-6 (“the Asserted Claims”) of the ’989 Patent under 35 U.S.C. § 102. Okereke also renders obvious the Asserted Claims under 35 U.S.C. § 103, alone based on the state of the art and/or in combination with one or more references identified in Samsung’s accompanying disclosure for the ’989 Patent.¹

To the extent Plaintiff alleges that Okereke does not disclose any particular limitation of the Asserted Claims of the ’989 Patent, either expressly or inherently, it would have been obvious to a person of ordinary skill in the art as of the priority date of the ’989 Patent to modify the Okereke reference and/or to combine the teachings of the Okereke reference with other prior art references, including but not limited to the present prior art references found in Exhibits 989-A-Y and the corresponding section(s) of charts for other prior art references for the ’989 Patent in a manner that would have rendered the Asserted Claims invalid as obvious.

With respect to the obviousness of the Asserted Claims under 35 U.S.C. § 103, one or more of the principles enumerated by the United States Supreme Court in *KSR v. Teleflex*, 550 U.S. 398 (2007) apply, including: (a) combining various claimed elements known in the prior art according to known methods to yield a predictable result; and/or (b) making a simple substitution of one or more known elements for another to obtain a predictable result; and/or (c) using a known technique to improve a similar device or method in the same way; and/or (d) applying a known technique to a known device or method ready for improvement to yield a predictable result; and/or (e) choosing from a finite number of identified, predictable solutions with a reasonable expectation of success or, in other words, the solution was one which was “obvious to try”; and/or (f) a known work in one field of endeavor prompting variations of it for use either in the same field or a different field based on given design incentives or other market forces in which the variations were predictable to one of ordinary skill in the art; and/or (g) a teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill in the art to modify the prior art reference or to combine the teachings of various prior art references to arrive at the claimed invention. It therefore would have been obvious to one of ordinary skill in the art to combine the disclosures of these references in accordance with the principles and rationales set forth above.

¹ Samsung notes that Plaintiff appears in many instances to be pursuing overly broad constructions of various limitations of the asserted claims of the ’989 Patent in an effort to piece together an infringement claim where none exists and to accuse a product that does not practice the claims. This claim chart may take into account Plaintiff’s overly broad constructions of the claim limitations. Any assertion that a particular limitation is disclosed by a prior art reference may be based on Plaintiff’s apparent constructions and is not intended to be, and is not, an admission that such constructions are supportable or proper.

Exhibit 989-Z**Invalidity Chart for U.S. Patent No. 10,698,989 In View of Okereke**

The citations to portions of any reference in this chart are exemplary only. For example, a citation that refers to or discusses a figure or figure item should be understood to also incorporate by reference that figure and any additional descriptions of that figure as if set forth fully therein. Samsung reserves the right to rely on the entirety of the references cited in this chart to show that the Asserted Claims are invalid. Citations presented for one claim limitation are expressly incorporated by reference into all other limitations for that claim as well as all limitations of all claims on which that claim depends. Samsung also reserves the right to rely on additional citations or sources of evidence that also may be applicable, or that may become applicable in light of claim construction, changes in Plaintiff's infringement contentions, and/or information obtained during discovery as the case progresses.

Claim	U.S. Patent No. 10,698,989	Exemplary Disclosure in Okereke
1 pre	A method comprising:	The Preamble is not limiting.
1A	receiving, at a smartphone, an identification (ID) code from a third-party trusted authority, the ID code uniquely identifying the smartphone among a plurality of smartphones;	<p>Okereke render obvious receiving, at a smartphone, an identification (ID) code from a third-party trusted authority, the ID code uniquely identifying the smartphone among a plurality of smartphones.</p> <p>For example, Okereke discloses a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device in the form of a serial number or SIM number and a private/public key process. Although, Johnson does not disclose the use of smartphone, it would be obvious to include it in this way.</p> <p><i>See, e.g.,</i></p> <p>“The establishment of mobile access to secure resources in accordance with the present invention can occur as shown in FIGS. 4 and 5. The proxy server can be provided with software designed in accordance with the present invention, and a thin client application can be installed and/or downloaded onto the user's desktop computer. The proxy server program then awaits the initiation of a request 210 from the desktop to establish secure wireless access capabilities</p>

Exhibit 989-Z
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Okereke

		<p>using the system of the present invention. In so doing, a unique identifier for the wireless product to be employed is passed as at 210 to the proxy server 125 program for authorization. The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other device capable of remote wireless communication. The unique identifier can be a serial number or SIM. number, for example. If the unique identifier is one which the proxy server program identifies as being acceptable, the proxy server program will send approval as at 220 to the desktop 140, which executes functionality to make a key exchange as at 225, such as, for example, a Diffie Hellman Key Exchange. This key is used to encrypt information sent to the server using AES (Advanced Encryption Standard). AES is an encryption algorithm used by U.S. government agencies for securing sensitive but unclassified communications. In the preferred embodiment, this key is used to encrypt communication between the desktop and the server. In another embodiment, this key is used as part of a shared secret between the server and the client. This shared secret is used to generate a session key. The new session key ensures that conversations cannot be eavesdropped if the key has been compromised. The shared secret eliminates the possibility of a man-in-the-middle attack.”</p> <p><i>Id.</i> at ¶25.</p> <p>“The desktop computer includes a memory, processor, user interface, keyboard and mouse as is commonly known, and is preferably connected to a local area network (LAN) 175 for communication and use of shared resources as is commonly known. The user may be provided with a system PKI certificate 180 and private key for use with the desktop computer, in order to access and communicate to the extent authorized by the network administrator.”</p> <p><i>Id.</i> at ¶24.</p>
1B	persistently storing biometric data and the ID code on the smartphone, wherein the biometric data is one selected from a group	Okereke discloses persistently storing biometric data and the ID code on the smartphone, wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan of a legitimate user.

Exhibit 989-Z
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Okereke

	consisting of facial recognition, a fingerprint scan, and a retinal scan of a legitimate user;	<p>For example, Okereke discloses using fingerprint to secure the device.</p> <p><i>See, e.g.,</i></p> <p>“In other cases, an additional form of authentication may be required, such as a user name and password, a smart card, or a fingerprint, for example.” <i>Id.</i> at ¶21.</p> <p>“The credential information or authentication measure can be something the user has (such as a swipe card), something the user is (such as represented by a fingerprint scan), or something the user knows (such as a password or pass phrase)” <i>Id.</i> at ¶26.</p>
1C	receiving, at the smartphone, scan data from a biometric scan using the smartphone;	<p>Okereke render obvious responsive to receiving, at the smartphone, scan data from a biometric scan using the smartphone.</p> <p>For example, Okereke discloses using biometric verification – including a fingerprint – to verify the user of the device. Although, Johnson does not disclose the use of smartphone, it would be obvious to include it in this way.</p> <p><i>See, e.g.,</i></p> <p>“The wireless device 165 is provided with a memory, processor, and input/output means as is commonly known. Using the session key, the user can then encrypt credential information, its PKI certificate 180 and private key, and forward this information to the proxy server 125 as at 230 in FIGS. 4 and 5. In one embodiment of the invention, the encrypted information is sent to the proxy server via secure IP network. The credential information or authentication measure can be something the user has (such as a swipe card), something the</p>

Exhibit 989-Z
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Okereke

		<p>user is (such as represented by a fingerprint scan), or something the user knows (such as a password or pass phrase). In one embodiment, the credential information is a user name and password. In another embodiment of the invention, the credential information is a random number generated by programming on the wireless device, wherein the number changes in predetermined time intervals and is synchronized with programming on the proxy server so as to always match the corresponding number maintained on the proxy server.”</p> <p><i>Id.</i> at ¶26.</p> <p>“In one embodiment of the invention, desktop software is used to authenticate the user to the CPS, register the wireless device with the CPS, facilitate the initial key exchange and transfer the certificate and private key to the server. When the user wishes to access a resource from the wireless device outside of the secure network demarcation line (102 in FIG. 3), they are prompted for a second means of authentication, which may be something the user has (such as a swipe card, synchronized password keychain or channel key, for example), something the user is (such as a fingerprint scan), or something the user knows (such as a password or pass phrase). In a preferred embodiment this second form of authentication is something the user knows. The CPS verifies both forms of authentication, locates the user's certificate and establishes a session.”</p> <p><i>Id.</i> at ¶32.</p>
1D	comparing, using the smartphone, the scan data to the biometric data;	<p>Okereke discloses comparing, using the smartphone, the scan data to the biometric data.</p> <p>For example, Okereke discloses using biometric verification – including a fingerprint – to verify the user of the device.</p> <p><i>See, e.g.,</i></p>

Exhibit 989-Z
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Okereke

		<p>“The wireless device 165 is provided with a memory, processor, and input/output means as is commonly known. Using the session key, the user can then encrypt credential information, its PKI certificate 180 and private key, and forward this information to the proxy server 125 as at 230 in FIGS. 4 and 5. In one embodiment of the invention, the encrypted information is sent to the proxy server via secure IP network. The credential information or authentication measure can be something the user has (such as a swipe card), something the user is (such as represented by a fingerprint scan), or something the user knows (such as a password or pass phrase). In one embodiment, the credential information is a user name and password. In another embodiment of the invention, the credential information is a random number generated by programming on the wireless device, wherein the number changes in predetermined time intervals and is synchronized with programming on the proxy server so as to always match the corresponding number maintained on the proxy server.”</p> <p><i>Id.</i> at ¶26.</p> <p>“In one embodiment of the invention, desktop software is used to authenticate the user to the CPS, register the wireless device with the CPS, facilitate the initial key exchange and transfer the certificate and private key to the server. When the user wishes to access a resource from the wireless device outside of the secure network demarcation line (102 in FIG. 3), they are prompted for a second means of authentication, which may be something the user has (such as a swipe card, synchronized password keychain or channel key, for example), something the user is (such as a fingerprint scan), or something the user knows (such as a password or pass phrase). In a preferred embodiment this second form of authentication is something the user knows. The CPS verifies both forms of authentication, locates the user's certificate and establishes a session.”</p> <p><i>Id.</i> at ¶32.</p>
--	--	---

Exhibit 989-Z
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Okereke

“The establishment of mobile access to secure resources in accordance with the present invention can occur as shown in FIGS. 4 and 5. The proxy server can be provided with software designed in accordance with the present invention, and a thin client application can be installed and/or downloaded onto the user's desktop computer. The proxy server program then awaits the initiation of a request 210 from the desktop to establish secure wireless access capabilities using the system of the present invention. In so doing, a unique identifier for the wireless product to be employed is passed as at 210 to the proxy server 125 program for authorization. The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other device capable of remote wireless communication. The unique identifier can be a serial number or SIM. number, for example. If the unique identifier is one which the proxy server program identifies as being acceptable, the proxy server program will send approval as at 220 to the desktop 140, which executes functionality to make a key exchange as at 225, such as, for example, a Diffie Hellman Key Exchange.”

Id. at ¶25.

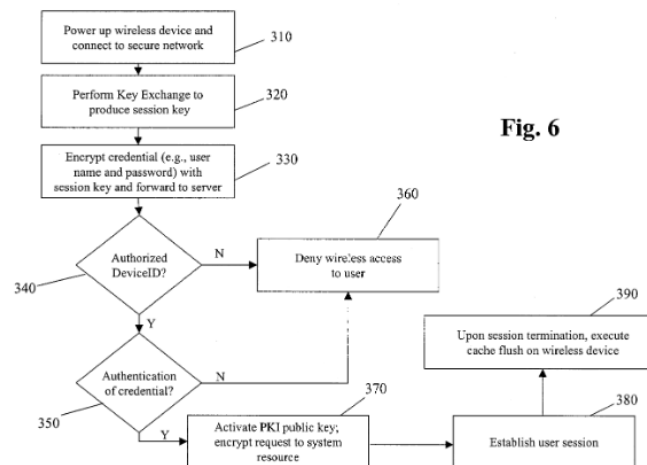
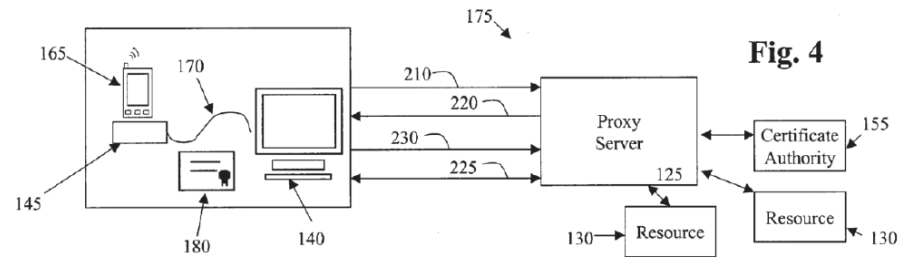


Exhibit 989-Z
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Okereke

		<p><i>Id.</i> at Fig. 6.</p> <p>“If the user is authenticated by the proxy server matching the device unique identifier with authorized device identifications as at 340, and the credential information is authenticated as determined at 350, the proxy server will activate the user's PKI public key and request the secure network resource for the user, as at 370.”</p> <p><i>Id.</i> at ¶28.</p> <p>“The user can ensure secure communication between the wireless device and the Certificate Proxy Server (CPS) in various ways, including physically connecting the device to the server, or connecting securely over a known trusted network. As the user's certificate and private key are securely transferred to the CPS, the unique network identifier for the user's wireless device (such as a SIM number) is registered with the server. This network identifier registration can also be done in a number of ways, including over the wireless network, or over a physical network.”</p> <p><i>Id.</i> at ¶30.</p>
1H	a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code	<p>Okereke discloses a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code.</p> <p>For example, Okereke discloses an access would be given only if the users or the devices are authenticated by the proxy server.</p> <p><i>See, e.g.,</i></p>

Exhibit 989-Z
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Okereke

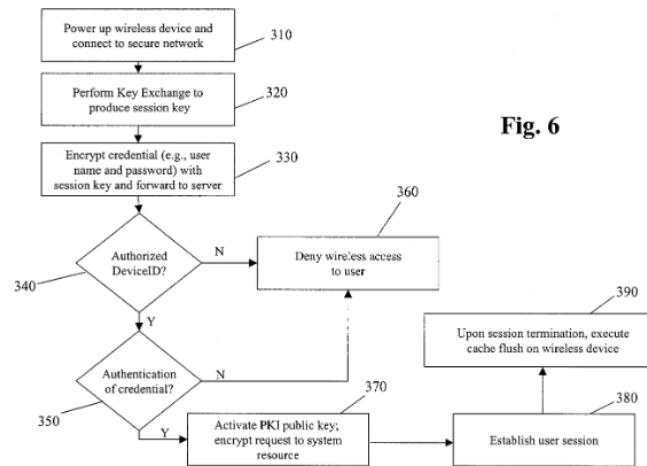


Id. at Fig. 4.

“The establishment of mobile access to secure resources in accordance with the present invention can occur as shown in FIGS. 4 and 5. The proxy server can be provided with software designed in accordance with the present invention, and a thin client application can be installed and/or downloaded onto the user's desktop computer. The proxy server program then awaits the initiation of a request 210 from the desktop to establish secure wireless access capabilities using the system of the present invention. In so doing, a unique identifier for the wireless product to be employed is passed as at 210 to the proxy server 125 program for authorization. The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other device capable of remote wireless communication. The unique identifier can be a serial number or SIM. number, for example. If the unique identifier is one which the proxy server program identifies as being acceptable, the proxy server program will send approval as at 220 to the desktop 140, which executes functionality to make a key exchange as at 225, such as, for example, a Diffie Hellman Key Exchange.”

Id. at ¶25.

Exhibit 989-Z
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Okereke



Id. at Fig. 6.

“If the user is authenticated by the proxy server matching the device unique identifier with authorized device identifications as at 340, and the credential information is authenticated as determined at 350, the proxy server will activate the user's PKI public key and request the secure network resource for the user, as at 370.”

Id. at ¶28.

“The user can ensure secure communication between the wireless device and the Certificate Proxy Server (CPS) in various ways, including physically connecting the device to the server, or connecting securely over a known trusted network. As the user's certificate and private key are securely transferred to the CPS, the unique network identifier for the user's wireless device (such as a SIM number) is registered with the server. This network identifier registration can also be done in a number of ways, including over the wireless network, or over a physical network.”

Id. at ¶30.

Exhibit 989-Z
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Okereke

1I	<p>wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.</p>	<p>Okereke discloses wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.</p> <p><i>See 1H.</i></p> <p>For example, Okereke discloses that access would be given applications of either computer software, a file (or both).</p> <p><i>See, e.g.,</i></p> <pre> graph TD 310[Power up wireless device and connect to secure network] --> 320[Perform Key Exchange to produce session key] 320 --> 330[Encrypt credential (e.g., user name and password) with session key and forward to server] 330 --> 340{Authorized DeviceID?} 340 -- N --> 360[Deny wire/less access to user] 340 -- Y --> 350{Authentication of credential?} 350 -- N --> 360 350 -- Y --> 370[Activate PKI public key; encrypt request to system resource] 370 --> 380[Establish user session] 380 --> 390[Upon session termination, execute cache flush on wireless device] </pre> <p style="text-align: center;">Fig. 6</p> <p><i>Id.</i> at Fig. 6.</p> <p>“If the user is authenticated by the proxy server matching the device unique identifier with authorized device identifications as at 340, and the credential information is authenticated as determined at 350, the proxy server will activate the user's PKI public key and request the secure network resource for the user, as at 370. If the device identification is not authorized, or the user's credential is not authenticated, access to the user will be denied as at 360. The proxy server</p>
----	--	---

Exhibit 989-Z
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Okereke

		will then receive the request for digital certificate and private key, and provide the previously stored digital certificate and key, which can then be validated by the certificate authority, and the user's session can begin.” <i>Id.</i> at ¶28.
2A	The method of claim 1, further comprising: Receiving a request for biometric verification, and	Okereke discloses receiving a request for biometric verification. <i>See</i> 1C-D.
2B	responsive to a determination that the scan data does not match the biometric data,	Okereke discloses responsive to a determination that the scan data does not match the biometric data. <i>See</i> 1C-D.
2C	indicating the smartphone cannot verify the scan data as being from the legitimate user, the smartphone does not send the ID code.	Okereke discloses indicating the device cannot verify the scan data as being from the legitimate user, the smartphone does not send the ID code. <i>See</i> 2B
3	The method of claim 1, wherein completing the transaction includes accessing an application.	Okereke discloses transaction includes accessing an application. <i>See</i> 1H.
4A	The method of claim 1, wherein the transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code	Okereke discloses wherein the transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code. <i>See</i> 1G-1H.
4B	includes the third-party trusted authority sending an indication that the third-party trusted authority authenticated the ID code to another party.	Okereke discloses includes the third-party trusted authority sending an indication that the third-party trusted authority authenticated the ID code to another party. <i>See</i> 1H.

Exhibit 989-Z
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Okereke

5pre	A smartphone comprising:	Okereke discloses a device. <i>See 1A.</i>
5A	a persistent storage having an input that receives an identification (ID) code from a third-party trusted authority, and biometric data	Okereke discloses a persistent storage having an input that receives an identification (ID) code from a third-party trusted authority, and biometric data. <i>See 1A.</i>
5B	wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan, of a legitimate user	Okereke discloses wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan, of a legitimate user. <i>See 1B.</i>
5C	the ID code uniquely identifying the smartphone among a plurality of smartphones	Okereke discloses the ID code uniquely identifying the device among a plurality of devices. <i>See 1A.</i>
5D	the persistent storage storing the biometric data and the ID code,	Okereke discloses the persistent storage storing the biometric data and the ID code. <i>See 1A.</i>
5E	the persistent storage having an output configured to provide a first set of biometric data and the ID code for use on the smartphone;	Okereke discloses the persistent storage having an output configured to provide a first set of biometric data and the ID code for use on the device. <i>See 1A.</i>
5F	a validation module, coupled to communicate with the persistent storage to receive the biometric data from the persistent storage,	Okereke discloses a validation module, coupled to communicate with the persistent storage to receive the biometric data from the persistent storage. <i>See 1D.</i>

Exhibit 989-Z
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Okereke

5G	the validation module having a scan pad to capture scan data from a biometric scan,	Okereke discloses the validation module having a scan pad to capture scan data from a biometric scan. <i>See 1C-D.</i>
5H	the validation module comparing the scan data to the biometric data to determine whether the scan data matches the biometric data; and	Okereke discloses the validation module comparing the scan data to the biometric data to determine whether the scan data matches the biometric data. <i>See 1D.</i>
5I	a wireless transceiver that,	Okereke discloses a wireless transceiver. <i>See 1G.</i>
5J	responsive to a determination that the scan data matches the biometric data,	Okereke discloses responsive to a determination that the scan data matches the biometric data. <i>See 1C-D.</i>
5K	sends the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority,	Okereke discloses sends the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority. <i>See 1G.</i>
5L	a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code,	Okereke discloses a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code. <i>See 1H.</i>
5M	wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a	Okereke discloses wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.

Exhibit 989-Z
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Okereke

	keyless lock, an ATM machine, a web site, a file and a financial account.	<i>See</i> 1I.
6	The smartphone of claim 5, wherein the ID code is transmitted to the third-party trusted authority over a network.	<p>Okereke discloses wherein the ID code is transmitted to the third-party trusted authority over a network.</p> <p>For example, Okereke discloses transmitting device identifier over the Internet.</p> <p><i>See, e.g.,</i></p> <p>“In a specific embodiment as shown in FIG. 4, the user is first provided with a network-connected device, such as a desktop computer 140, along with one or more docking stations 145. One or more wireless-capable devices 165 may be docked in the docking station for two-way communication with the desktop computer as indicated at 170. The desktop computer includes a memory, processor, user interface, keyboard and mouse as is commonly known, and is preferably connected to a local area network (LAN) 175 for communication and use of shared resources as is commonly known.”</p> <p><i>Id.</i> at ¶24.</p> <p>“The proxy server can be provided with software designed in accordance with the present invention, and a thin client application can be installed and/or downloaded onto the user's desktop computer. The proxy server program then awaits the initiation of a request 210 from the desktop to establish secure wireless access capabilities using the system of the present invention. In so doing, a unique identifier for the wireless product to be employed is passed as at 210 to the proxy server 125 program for authorization. The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other device capable of remote wireless communication. The unique identifier can be a serial number or SIM. number, for example.”</p> <p><i>Id.</i> at ¶25.</p>

Exhibit 989-Z
Invalidity Chart for U.S. Patent No. 10,698,989 In View of Okereke